LEARNING MADE EASY

# Managed Detection & Response (MDR)

for dummies®
A Wiley Brand

Maximize internal resources

Improve compliance through reporting

Accelerate security program maturity

Cloud9™
DATA SOLUTIONS

James Sullivan

# Managed Detection & Response (MDR) For Dummies®

Published by
**John Wiley & Sons, Inc.**
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com



ISBN: 978-1-119- 86978-8 (pbk); ISBN: 978-1-119- 86979-5 (ebk)

## Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

**Project Manager:** Jen Bingham

**Acquisitions Editor:** Ashley Coffey

**Editorial Manager:** Rev Mengle

# Table of Contents

# Introduction

The IT security landscape is rapidly shifting. New threats and attack strategies pop up every year, and cybercriminals are finding new ways to turn a profit in cybercrime. Security threats are more sophisticated than ever, and many organizations are having a hard time developing the strong security posture they need to stay healthy.

There is a security professional shortage right now, meaning hiring and retaining a team that's ready for action is difficult. Modern security tools require experts to manage and fully leverage them, and security policies should be constantly evolving to meet current security needs.

Services like managed detection and response (MDR) are a strong addition to the security solutions market and offer tempting value propositions for many organizations. These services provide the security expertise and technology required to develop comprehensive security infrastructures, can adapt to shifting threat landscape conditions, and operate on a highly available schedule.

## About This Book

MDR services were only recently introduced to the security solutions market and are a modern iteration of older security services, namely managed security service providers (MSSPs). This book begins with an overview of the current security landscape, including discussions on popular security solutions that you might have heard about or are already using at your organization.

Next, the book dives into what makes MDRs stand out, what services and advantages they provide, and some things to look out for when finding the service that's right for your organization.

# Icons Used in This Book

This book uses a few special symbols to point out important points to remember, general tips, or touch on a technical subject not covered in the main text. Here is the list of special icons used in this book.

REMEMBER

This symbol is used to point out an important takeaway from a given section. This might be an idea crucial to understanding a topic or a discussion point that may show up later in the book.

TIP

These are useful bits of info that should help flesh out your understanding of MDR or the security landscape in general.

TECHNICAL STUFF

This icon expands on technical points that aren't explicitly covered in the main body of a section.

WARNING

This icon marks information that can help you avoid trouble or at least give you a heads-up.

IN THIS CHAPTER

- How cyberthreats are changing
- The cyberthreats impacting organizations the most
- Telltale signs of a cyberattack
- Exploring the modern cybersecurity toolbox

# Chapter 1
# Cybersecurity Is Evolving

This book will cover a lot, so it seems smart to start from the ground floor. What's happening in cybersecurity right now? The short answer: a lot. This chapter goes over how cyberthreats are changing, how these threats are impacting organizations, and what sorts of solutions are available to defend against them.

Before jumping into the meat of the book, one quick semantic note: The term *cybersecurity landscape* pops up sometimes in these pages, which may seem overly general. However, each component of the landscape (current threats, security solutions, work environments, and so on) pushes and pulls on the others. The term is a recognition that any one aspect of the landscape doesn't exist in a vacuum. So, with that in mind, what does the cybersecurity landscape look like right now?

## Cyberthreats Are Changing

The nature of cyberthreats has changed a lot in the past five years. Not only are the types of attacks different, but the people carrying out attacks, the targets, and the ways in which cybercriminals are able to support themselves and benefit from cybercrime are all shifting.

REMEMBER

The push to work from home, the explosion of connected devices, the increasing relevance of cryptocurrencies, the threat of cyberespionage, and the ubiquity of data collection across industries are all factors in the shifting landscape. These may be some of the driving forces behind change in the current cybersecurity landscape, but there will be new forces next year, and the year after, and so on. If there is one thing you can take away from this section, it should be that a successful security program doesn't just provide the tools to deal with existing threats but also has the capability to deal with new and emerging threats down the road.

## Nation-state actors changed the game

State-sanctioned espionage and sabotage have existed as long as the nation-states that carry them out. Computer technology happens to be the most recent battleground for such activity. However, because of the sensitive nature of international politics, it's often difficult to call it out.

A recent incident in this realm is the 2020 discovery of the SolarWinds attack. This incident involved malicious code being spread across multiple U.S. government agencies that was undetected for months. Impacts of the attack are still felt today, and in the end, the attack was largely successful. There is a strong indication that the Russian government sanctioned this attack, or at least supports the group that carried it out.

WARNING

One of the primary issues with state-sanctioned cyberthreats is that there is little-to-no recourse after an attack. As these attacks are obviously between political adversaries, there are almost never legal repercussions for the perpetrators.

Additionally, the response to such state attacks is controlled by the governments themselves and not the private sector or contracted organizations directly impacted.

The only thing these organizations can do is prepare for and protect themselves against the attacks. Whether it's manufacturing, healthcare, finance, transportation, or any number of other industries, disruptive attacks on an organization's systems can potentially benefit state adversaries.

Even nation-state-supported attackers are not industry agnostic.

## New ways to make it as a cybercriminal

Another factor changing the cybersecurity landscape is cryptocurrency. For starters, currencies like Bitcoin provide cybercriminals with new, safer ways to get paid. Not only are these transactions harder to trace, but they're also easier to offload.

The rise of cryptocurrency has also increased the demand for compute resources. There is now a great reason for cybercriminals to try to gain unauthorized access to an organization's compute resources, such as central processing units (CPUs) and graphics processing units (GPUs), because using these resources to mine for currency provides a direct monetary benefit to the cybercriminals.

WARNING

Every new exploit or point of access is an opportunity for a cybercriminal, and the fact that there are more reasons than ever to break into private and public systems means nefarious activity won't be slowing down anytime soon.

# Current Threats Facing Organizations

One of the largest problems organizations run into when constructing and maintaining a comprehensive security program is the sheer number of potential threats. Malware, ransomware, business email compromise, phishing schemes, and distributed denial-of-service (DDoS) attacks are all threats facing organizations, and each of them requires different types of security coverage.

This section breaks down some of the most common cyberthreats affecting organizations, talks about what they do, and explains how they can affect operations.

## Malware and ransomware

28 percent of all reported cyberattacks were malware incidents. In the simplest terms, malware is a malicious piece of software that disrupts or exploits areas like business operations or compute resources.

Ransomware is a kind of malware that is used to alert an organization that its resources have been compromised. The attackers then usually demand money in return for restoring regular operation of a stolen service or resource. This can involve disrupting operations, such as shutting down a business-critical system, or stealing customer data to either ransom back to an organization or sell to others.

REMEMBER

There are many ways malware can enter an organization's systems. Here are a few of the most common methods of introducing malicious code into a system:

- Network traffic
- Software exploits
- Downloaded files containing malicious code
- Using infected applications

Cybercriminals are smart and creative, so the ways malware can enter your organization change constantly.

## Phishing and the expanding attack surface

Phishing is the practice of sending counterfeit emails to lure recipients into clicking compromised links or downloading malicious files onto their machines. The code attached to those downloads or links can then infect the person's device, and potentially get into an organization's internal system.

With remote work on the rise, it makes sense that phishing attacks are more popular than ever. So much communication between co-workers happens via email, with documents transferred between colleagues. Attackers can take advantage by send-ing emails that look urgent, such as a URL that supposedly leads to updated access to internal systems or business-critical docu-ments that must be downloaded. Cybercriminals are finding new ways to trick users into clicking on malicious content every day, and organizations need to protect themselves.

## Attacks are more sophisticated than ever

With expanding attack surfaces, more complex internal systems, and new ways to benefit from cybercrime, attackers are driven to develop new strategies and find new weak points in modern security programs. A prime example of this is the rise in phishing schemes.

New ways to impersonate reputable organizations through email are thought up every day. Cybercriminals will also shift tactics based on current events, such as the rise in fake healthcare information emails during the COVID-19 pandemic.

Another security challenge is the increasing use of third-party software for regular business operations. Attackers are finding more ways to compromise this kind of software and infiltrate customer systems once the third-party solution is in place.

# What Does a Comprehensive Security Program Look Like?

So far, we've covered many of the security challenges facing organizations today. But what can they do about them? There are three main considerations that will influence the success of a security ecosystem: technical challenges, operational challenges, and management challenges. Each of these props up a comprehensive security program. Although these three factors offer different challenges, they support each other and are all needed to defend against active and emerging threats.

## The technical side

Think of the technical side as the first line of defense. It's where attackers will first run into problems accessing your systems and, in a perfect world, would be where all attackers are stopped in their tracks. The technical side of a security ecosystem includes:

- Access controls
- Identity and authentication management tools
- Intrusion detection tools
- Database and network protection

These security tools cover potential holes leading into an organization's systems and are designed to filter and gatekeep the users and information entering and exiting private environments.


TIP

There are purpose-built third-party tools for each one of these security considerations, but cobbling together a Frankenstein's monster of security solutions rarely works out. Not only do different tools often need to communicate with one another, but there are a slew of operational challenges that come with a self-constructed security ecosystem.

Luckily, there are many packaged security solutions that include tools for different security tasks. While there isn't a one-size-fits-all security solution, the modern security market has lots of options available to suit any organization's specific needs.

## Security operations

Operational considerations combine day-to-day security challenges with threat detection and remediation responsibilities of an organization's security operations team. Operational challenges include:

- Employee security training
- Incident investigation
- Information integrity
- Capability to detect real threats versus false positives
- Incident response planning

Some security solutions that offer suites of security tools aim to marry technical and operational tools to ease the burden on both aspects of the ecosystem. These solutions are a great way to get the most bang for your buck and lighten the load on management personnel.

## Managing the security program

Management considerations are more about big picture stuff. Managing a security ecosystem should involve lots of planning and assessment of current procedures, all in the hope that when a security threat gets through (because that happens), there are systems in place to deal with it. Management challenges include:

- Risk assessment
- Security policies
- System monitoring
- Security plan implementation

This side of the security ecosystem is really about maintaining a bird's-eye view on the procedures and policies in place, developing strategies to improve them, and learning from mistakes when those procedures fail.

TIP

This last point is especially important. When an attack gets through or policies don't work as planned, don't get discouraged. These are learning opportunities and can be valuable in preparing for future security threats.

# Recent Incidents

Cyberattacks are frequent, and there are too many breaches for each one to be covered in the main news cycle. Even security incidents that impact millions of people may not get covered by large news organizations. This section covers some of the most recent security breaches, talking about what went wrong and what could have been done to prevent, or at least mitigate, the damage. We will focus on attacks in the healthcare and manufacturing industries, but cyberattacks are not exclusive to these two markets. Organizations in energy, transportation, agriculture, finance, and many other industries are all potential targets for attackers.

## Healthcare

According to the *HIPAA Journal*, there were 52 IT security breaches in U.S. healthcare systems in July 2021 alone. That's almost two breaches every day. Ransomware and phishing attacks made up the vast majority of these incidents.

The Orlando Family Physicians practice in Florida is one such recent breach. The healthcare group stated that in April 2021, a phishing email tricked an employee into disclosing some private account information. More employees fell for the phishing scheme, and the attackers soon had the protected health records of almost half a million people.

The attackers' goal was not the health records themselves but to eventually extort the medical practice for money. Orlando Family Physicians hired an outside group of security forensic specialists to help investigate and resolve the situation, but a lot of damage had already been done.

Although it seems easy to point the finger at the employees who fell for the phishing emails, there are security tools and procedures the medical practice could have used to prevent such a large data breach. For starters, proper infrastructure monitoring, with eyes on networks, endpoints, account logins, clouds, and more, could have significantly reduced the impact of this attack. From a management perspective, incident response planning and testing, risk assessments, and tabletop exercises should have been carried out to identify weak spots in the security ecosystem.

While employee security training is also important, there are many policies and security infrastructure decisions that could have been made differently to save the logistical headache and dangerous data compromises brought by the attack.

## Manufacturing

Manufacturing is another industry that is especially at risk. It's been one of the most attacked industries for several years, with some estimates showing that one in four manufacturing companies are attacked every week. That's a shocking number and reinforces the need for comprehensive cybersecurity coverage.

In February 2021, Canadian airplane manufacturer Bombardier suffered a data breach caused by a vulnerability in a third-party web server. Luckily, this software exploit was limited to a single server and only affected 130 employees. Although this is a relatively small data breach, this is the kind of incident that can easily spiral out of control if not kept in check.


The kind of incident Bombardier experienced is called a zero-day attack. A zero-day attack is one where a bad actor exploits a software vulnerability that is either unknown or hasn't been patched yet. This kind of breach can be especially harmful, as shown by the 2013 Yahoo! incident that impacted over 3 billion user accounts.

Like the healthcare breach discussed earlier, continuous monitoring is crucial to detecting and responding to data breaches. Effective security programs should include plans to detect and halt data exfiltration, even from third-party vendor resources.

Additionally, regular security audits can prevent an attack like this from happening, or at least lessen the impact when one gets through.

# The Current Security Solutions Landscape

This section takes a look at some of the solutions organizations can use to stop security threats.

## MSSP, SIEM, and the alphabet soup of security solutions

SIEM, SOAR, NDR, EDR, MSSP, MDR, XDR. This mess of letters is just the tip of the iceberg when it comes to the security solutions market.

SIEM, or security information and event management, has been around for a while. The main purpose of SIEM tools is to collect and process event data across an organization's security ecosystem. SIEM is the king of security alerts, which can be useful for certain customers, but most organizations simply don't need a mountain of log data and instead should focus on streamlining security operations. Although SIEMs can be powerful monitoring tools, they can often lead to alert fatigue by sending too many benign security alerts.


TIP

You don't have to remember every security acronym to find the solution that's right for your organization. Just know enough to find the solution that fits your organization's specific needs, and you can forget the rest.

Another popular security tool is security orchestration, automation, and response (SOAR). SOAR solutions focus on analyzing event data by folding in some SIEM functionality and using that data to respond quickly to incidents and develop response plans to future security events.

SOAR solutions provide a lot of functionality to security teams, but yes, it requires a robust security team to get the most out of them. The information and toolbox provided by SOARs are designed for security professionals, which require a lot of overhead for small to midsize organizations.

Other, more focused security solutions include endpoint detection and response (EDR) and network detection and response (NDR). Tools like these are designed specifically for monitoring and alerting on suspicious behavior in their areas. NDRs and EDRs can often be integrated with more big picture solutions like SOAR, but still require the expertise of seasoned security staff to function properly.

## MDR

Managed detection and response (MDR) is a modern security solution that packages security tools for your internal systems with access to security professionals. The biggest difference between MDR and other security products and services is the human element. MDR solutions will often integrate with your existing IT infrastructure, including networks, endpoints, logs, users, and clouds, and provide security and IT teams with visibility of those systems.

A similar security solution on the market is managed security service provider (MSSP). MSSP is a legacy service that provides organizations with tools to monitor and control access and traffic within an IT infrastructure. The crucial difference between MSSPs and MDR solutions is that MSSPs are focused on preventing attacks from happening, while MDRs monitor and defend against attacks and also aid in the response to attacks that do get through.

Both MDR and MSSPs are built for organizations that either don't need or can't support full security operations teams. While MSSPs can be useful, MDR solutions usually provide deeper security coverage for businesses.

IN THIS CHAPTER

- An overview of MDR solutions
- Different tools on the cybersecurity market
- MDR's place in the current market

# Chapter 2
# What Is MDR?

The modern security solutions market is broad and opaque. There are many kinds of security products and services, there is a lot of functionality overlap between them, and most have names that sound helpful and like something you absolutely need. It's a lot to keep up with, even for some pros who have been in the field for years. This chapter goes over what managed detection and response (MDR) is, what it offers, some of the other popular security solutions available, and how MDR fits in with the broader security solutions market.

## Managed Detection and Response

MDR is more a security service than it is a security tool. The words "detection and response" sound like the most important part of the acronym, and those are the meat and potatoes of any good security infrastructure, but what sets MDR apart is how the solution is managed.

MDR service providers offer businesses access to in-house security experts who take care of monitoring, alerting, investigating, response plans, and more. MDR providers' detection and response tools are integrated into an existing IT infrastructure so the security pros can detect and respond to security threats.

MDR solutions are both for small to midsize organizations that can't support a full staff of security operations employees and larger organizations that wish to supplement their existing security solutions. MDR is a strong option for many organizations, but it's important to keep in mind that not all MDRs are created equal. At their core, MDR solutions offer integrated security tools that are monitored and managed by the provider's security professionals, but there can be key differences between solutions.

# What Does It Bring to the Table?

There are some very specific IT security challenges that MDR can help organizations tackle.

## Improving the incident detection and response lifecycle

The detection and response lifecycle encompasses finding security threats, containing and eradicating them, repairing any damage done by them, and assessing how the threats got through defensive tools in the first place. Ideally, the lifecycle should be constantly evolving. Attack trends and techniques are always changing, and so should the detection and response lifecycle. There are two important metrics for determining the general success of an organization's threat detection and response lifecycle: MTTD and MTTR.

Mean time to detect (MTTD) and mean time to respond (MTTR) are critical metrics for measuring the success of any IT security program. MTTD is the average time it takes for an organization's security team, or security service's team, to detect an infiltration. Similarly, MTTR is the average time it takes to respond to those threats. It takes time to develop accurate MTTD and MTTR values, and hopefully they trend toward zero over time.

MDR services work to lower MTTD and MTTR by providing comprehensive endpoint, network, log, and cloud monitoring, risk assessment and response plans, and using threat data from previous attacks to evolve those strategies. Because MDR services are managed by security pros, the threat detection and response lifecycle is able to adapt to emerging threats and streamline existing security processes to lower MTTD and MTTR.

REMEMBER

The threat detection and response lifecycle should always be evolving. New processes should be put in place when needed, policies changed based on current conditions, detection and remediation tools tweaked to suit an organization's current needs, and so on.

## Low barrier to entry

One of the biggest security challenges facing organizations is simply finding and financially supporting people with the know-how to run their security operations. Picking up a network detection and response (NDR), an endpoint detection and response (EDR), and a security information and event management (SIEM) solution is easy enough. Integrating and operating those solutions is another story.

TIP

A lot of expertise needs to be put into running these tools to fully leverage them, so at least a small security team is a must if this is the path an organization wants to go down. Security teams are expensive and add a lot to the management overhead at any organization, so many small to midsize operations just can't support this kind of investment.

MDR has a much lower barrier to entry. MDR is a service, meaning an organization can sign up and get walked through the integration and management process. The processes, defensive tools, and security policies that get set up are then managed by the service itself, with minimal client interaction and management.

This low barrier to entry means more organizations have access to the security operations program they need. Cybersecurity threats are more prevalent than ever, but luckily, many comprehensive security options are within reach.

## Expertise matters: The human element

This book has already mentioned the importance of security professionals when trying to operate and manage the security solutions available today. IT infrastructure is a complex beast, and so are the tools needed to defend it.

MDR services often integrate security tools like EDR and NDR into a client's existing infrastructure. Normally, these tools would require an in-house security team to operate them, but one of the greatest advantages of MDR is that it provides those security personnel.

REMEMBER

As a security service, MDR offers the tools needed to defend an IT infrastructure along with the people required to manage and operate it. More than that, having a group of security pros a phone call away for security questions can be a boon. It offers easily accessible expert guidance, answers to any security-related questions, and peace of mind.

# The Security Solutions Market

A quick look at the security solutions market reveals an absolute mess of acronyms. While each type of security solution offers something unique and can fit different needs, there is a lot of coverage overlap between some offerings that can make navigating the market tricky. This section discusses some of the most popular IT security solutions, talking about their use cases and how they fit into the larger security solutions market.

## SIEM

SIEM is a technology platform that focuses on security logging and alerting. SIEMs integrate with an organization's existing security infrastructure, specifically by monitoring existing endpoint and network monitoring tools. The SIEM will then aggregate and log security data from these sources, alerting security teams or administrators when suspicious behavior is detected.

Here are some of the biggest advantages of SIEM solutions:

- First, managing security data from separate data sources, such as EDRs and NDRs, is a lot of work. It also forces employees to manage a lot of useless information. SIEMs often provide some analysis features along with data aggregation to streamline this process.
- The second big pro of SIEM solutions is specifically for regulation-heavy industries that have steep security audit and logging requirements. Healthcare and financial services organizations often require large amounts of log data to comply with government regulations on their respective industries.

This second advantage, it turns out, is also SIEM's biggest issue. While mountains of log information are great for certain organizations, it's more trouble than it's worth most of the time. SIEM

solutions have a reputation for inducing alert fatigue on the people in charge of security alerts. This leads to employee burnout and potentially missing actual security threats.

REMEMBER

SIEMs are still an important part of modern security infrastructures, but most organizations don't have the resources to fully tune and leverage them.

SIEM solutions are battle-tested security products that have been around for years, and they are evolving. However, in the modern security landscape, getting the full potential out of SIEM products usually involves investing in other security solutions to help manage the waves of alerts.

## MSSP

Managed security service providers (MSSPs) are another popular security solution, and it's easy to see why. Like MDR services, MSSPs are a security service (it does what it says on the tin) that helps clients by monitoring their IT infrastructure and removes the barrier to entry by providing their own security tools to monitor a client's internal systems.

The first pro of MSSPs is that they don't require a dedicated in-house security team because they're managed services. This cuts costs and eliminates the management overhead of fielding a team of security professionals. The second pro of MSSPs is that, like SIEMs, these services provide strong internal system monitoring.

But, and I'm sure you saw this coming, MSSPs have downsides, too. Most MSSPs have limited visibility of a client's IT infrastructure. Security threats have evolved, and security solutions that were simple and effective are now, unfortunately, just simple. In addition to suffering from limited visibility, MSSPs often lack attack response and remediation services. An MSSP client is using this service to cover its security needs, but the threat lifecycle doesn't end with an alert. Clients need action plans and threat remediation capabilities to say they have a comprehensive security infrastructure. For more on this topic, see Chapter 1.

## XDR

Extended detection and response (XDR), like MDR, is a relatively new addition to the security solutions market. XDR solutions often include powerful detection and response tools that marry

NDR and EDR capabilities while also providing modern security tools like machine learning-driven analytics.

The first pro of XDR solutions is that they enable fine-grained visibility into endpoints, networks, logs, and sometimes cloud resources. The second pro is that XDR platforms usually play well with existing security tools, even increasing their value by aggregating the security information they're outputting.

WARNING

If your organization has a small to nonexistent security staff, XDR is off the table. XDR platforms require a full security operations team to properly manage.

The biggest problem with XDR is its complexity. XDR solutions, without question, require in-house security teams to operate and manage. XDRs need an existing security infrastructure and really serve to increase the value and effectiveness of a security team that's already in place. In the end, XDR is a solution tailored to large organizations and isn't suitable for most customers.

## How does MDR fit?

The short answer is that MDR fits for a lot of organizations. The most obvious comparison is with MSSPs, but MDR addresses MSSPs' issues by providing the fine-grained visibility of specialized detection and response products while also aiding in security event remediation and risk assessment and developing and executing response plans.

MDR solves many issues presented by SIEM and XDR solutions. As a managed service, MDR providers analyze security alerts for the client so they only get the alerts that matter. Additionally, MDR services provide threat response support, something missing from every SIEM offering.

REMEMBER

MDR is a service, not a single tool. It provides a range of capabilities, and the security pros working at the MDR service providers are available to help walk organizations through how the service can integrate with an existing security ecosystem.

MDRs also remove the steep barrier to entry of XDRs while retaining the fine-grained visibility and remediation tools. The bottom line is that MDR services often have access to cutting-edge security tools without the cost of maintaining and operating those tools in-house.

IN THIS CHAPTER

- Common organizational barriers faced by today's organizations
- Security technology hurdles
- How MDR addresses common challenges

# Chapter 3
# Organization Pain Points: Why Look for an MDR?

Although comprehensive security coverage is vital to the health of any organization, many still face trouble finding the tools that fit their budget and management restrictions while also meeting security needs. This chapter examines some of the most common problems organizations face when looking to strengthen their IT security posture and how managed detection and response (MDR) services can help overcome those challenges.

## Organizational Challenges

This book splits security infrastructure adoption challenges into two broad categories: organizational challenges and technological challenges. Organizational challenges include building security operations teams, industry regulation requirements, and security response process issues. Each of these topics presents different problems, but it ultimately comes down to finding, hiring, and retaining the right people to support a security infrastructure.

## The SecOps problem

Security operations (SecOps) is the marriage of security and operation management. It's a philosophy that aims to increase operational efficiency and security coverage, while leaving teams agile enough to adapt to changing market conditions.

Unfortunately, building a successful SecOps team is harder than it sounds because there is a shortage of available cybersecurity talent. This statement isn't a surprise to most because a 2021 analysis from the Information Systems Security Association found 57 percent of respondents said that the lack of available security workers had impacted their organizations. Also in this study, 95 percent said this workforce shortage has stayed consistently bad for years.

WARNING

This security pro shortage not only means it's hard to build a security team, but it also means the market is more competitive than ever. After hiring cybersecurity workers fresh out of school, training them, and incorporating them into the SecOps infrastructure, it's not uncommon to lose them to higher paying organizations. Security workers are in such high demand that they can often ascend pay bands too fast for small to midsize organizations to keep up.

Security services like MDR are an obvious solution to this problem. They provide the expertise and security infrastructure management of a fully staffed SecOps team without the cost and hassle of hiring and maintaining one.

## Compliance and regulation requirements

Industries with long histories of regulation like financial services and healthcare are no longer the only sectors with steep compliance requirements. New data storage-related legislation and visibility requirements are enacted each year, so there is a lot to keep up with. This is especially true if the organization serves an international client base.

Take a look at some of the most commonly encountered compliance requirements and who needs to comply with them:

- **HIPAA:** U.S. law regulates patient data for any healthcare entity operating within the United States.
- **Payment Card Industry Data Security Standard:** This standard regulates customer financial privacy and is a standard across the credit card industry.
- **General Data Protection Regulation:** This personal data privacy compliance standard is mandated by the European Union. Any organization holding EU citizen data must comply.
- **California Consumer Privacy Act:** This personal data regulation applies to any entity using the data of California residents.

Many organizations have more than one compliance standard to worry about, and keeping track of the data storage, security log, and attack incident audit requirements requires a lot of know-how to properly deal with. Complying with legal and industry standards isn't a place to cut corners. There are very few instances where getting a personalized letter from a governing body is a good thing.


TIP

Again, the access to security professionals provided by MDR services helps overcome this challenge. A select few MDR service providers offer risk assessments and penetration testing and have teams of people who know how to navigate compliance and regulation issues.

## Undocumented processes in the event of an attack or breach

Part of operations management is documenting incidents and learning from them. Organizations can learn a lot from attacks, and threat incidents can inform tweaks and updates to existing policies and processes. There are two primary hurdles preventing organizations from implementing proper incident reporting procedures.

First, comprehensive attack reports require fine-grained visibility and alerting for all relevant systems, including cloud, networks, and endpoints. There are many specialized endpoint and network detection tools available on the market to inform reporting, although cloud is more difficult to monitor. This part of the

challenge is more related to the technological hurdles. (For more about this, see the next section.)

The second major barrier to proper documentation procedures is the staff needed to process, interpret, and investigate the incident data. Learning from an attack can't happen without people deciphering why the attack happened and how it could have been prevented. Again, this is a multifaceted issue: security staff shortage, security staff retention problems, high operational costs, and so on.

A facet of MDR services is the information gathering and interpretation they offer. The security pros on the other end of the line have the visibility — thanks to the deployed security tools — and knowledge to see what's happening and why.

# Technical Challenges

The other side of this problematic coin is the technology challenge. Most modern security tools are expensive and difficult to manage — the ones that are easy to use lack the monitoring capabilities needed for full security coverage. Plus, unfortunately, cutting-edge tech just isn't enough to prevent attackers from getting in. This section goes into more detail about each of these challenges and how MDR can provide relief in these areas.

## Security tools are hard to maintain

The first technical barrier new security tool adopters will likely run into is just how difficult security solution deployment, integration, operation, and maintenance is.

The complexity of many security tools means specialized certifications are needed to properly operate and maintain them. The IT security market isn't monolithic, and different tools have different operating procedures. Target-specific detection and response tools like network detection and response and endpoint detection and response must be configured for an organization's systems, tested, and integrated into orchestration or higher-level monitoring tools such as extended detection and response (XDR).

The big picture tools, like XDR and security orchestration, automation, and response, often have customizable dashboards, include menus within menus, and require regular tweaking to fit current security needs. While these are powerful tools, getting the most out of them demands expertise that is expensive and hard to come by.

MDR services provide that expertise, along with many of the tools and security capabilities themselves. Security operations are handled by the service so clients can put more focus on other business-critical operations.

## Lack of visibility across organizations and tools

Lack of visibility across systems is one of the biggest security challenges facing organizations today. There are three primary reasons why true visibility is becoming more important and more difficult to attain:

- Advancements in cyberattacks require fine-grained visibility and monitoring.
- Visibility is needed for more user devices than ever with the push to work from home.
- Cloud services and tools, which also require monitoring, are increasingly popular.

Broad and deep visibility capabilities are important because attackers made them important. Alerts for run-of-the-mill suspicious network traffic and unauthorized logins don't cut it anymore. Bad actors are constantly finding new ways to infiltrate and gain control of internal resources. These new methods can involve small packets of data, or discreet lines of code in seemingly benign software. True visibility means having the ability to see the small, unexpected problems, not just the big, obvious ones.

WARNING

Although the great work-from-home migration is a sensible evolution of the modern workplace, it presents a slew of new security challenges. The most pressing is the expanded attack surfaces. Each new device and each new user connected to internal systems are new points of entry for cybercriminals.

Phishing attacks are wildly popular among attackers now, and it doesn't seem like just a fad. Phishing emails are an effective

way to grab login or authentication information from employees, contractors, and partners, as well as introduce malicious software into internally connected devices. Detecting suspicious activity as quickly as possible is one of the best ways to prevent damage from phishing attacks. Scam emails are becoming more sophisticated, not just in their capability to trick users but also in the ways they exploit target systems.

Visibility is crucial to defend expanded attack surfaces, and the cloud is part of that. Cloud adoption has been on the rise for years, meaning each year more targets and points of entry are introduced to attackers. Comprehensive monitoring capabilities include the capability to detect data exfiltration from cloud databases at a fine-grained level. It also detects suspicious communication between cloud services, as well as other activity that is difficult to pinpoint.


REMEMBER

Cloud visibility is a common weak point in modern security ecosystems. The cloud adoption rate is high, and it is hard for security trends to keep up with it. A security program should be able to evolve with the threat landscape.

Some specialized tools, such as XDRs, can address these challenges, but this loops back to the operational issues discussed before. Modern MDR services, on the other hand, provide the tools to enable visibility and the expertise to understand and operate them.

## Technology alone can't deter motivated attackers

Attackers are intelligent, determined, and creative. This means that any set-it-and-forget-it security technology simply won't keep them out. Even with security automation, machine learning-driven analysis, and other modern IT security techniques, cybercriminals will find a way to get around defenses without human intervention.

There are plenty of great IT security tools and solutions on the market today, but as we've already gone over, these come with serious cost and staffing problems. Without experienced security

staff working behind the scenes, security tools are no better than a line of scarecrows. It might look a little frightening at first, but it doesn't prevent determined, problem-solving humans from getting in.

REMEMBER

People are the foundation of a good security program. If you don't have experienced security staff in your organization to leverage security tools, then attackers will not have much trouble getting in.

In this light, MDR services are an accessible way to fight fire with fire. Security professionals at these service providers are just as intelligent, determined, and creative as the attackers, and they have access to the cutting-edge tools that stand the best chance of stopping threats. Additionally, people learn from mistakes. Machines don't. The human element also means that attacks that do get through become resources for developing future security policies, not just threat events that damage internal systems.

IN THIS CHAPTER

- A discussion of MSSP, an entry-level, legacy security service
- SIEM, security solutions providing visibility but limited analysis
- How MDR integrates security silos and provides full analysis

# Chapter 4
# MDR, MSSP, and SIEM: Which Is Right for You?

If it feels like every advance in infosec is accompanied by a new acronym or abbreviation, you are obviously paying attention. Today you have to wade through a few key terms for security services to understand your options for security solutions and what each one brings to the table. Three important ones are MSSP, SIEM, and MDR. This chapter goes over what each of these security offerings provides, what clients can expect to manage after adoption, and how managed detection and response (MDR) helps solve a lot of the issues presented by the two older solution types.

## MSSPs: Managed Security Service Providers

MSSPs are services that allow you to outsource some of your information security workload, especially around monitoring and preventing attacks from happening in your security systems. For example, an MSSP might manage your firewall configurations, make sure your antivirus software is up to date, and perform regular vulnerability scans of your applications.

## Entry-level security

Most organizations are very good at their core competencies and not so good in other areas. Retailers are good at selling things. Healthcare professionals are good at healing. Financial services companies are good at managing money. Information security is a broad and demanding field, and it's hard to get everything right all the time.

REMEMBER

MSSPs can help organizations with security by taking over some of the security workload that every organization needs to do. For example, an MSSP may be tasked with securing a company's network and evaluating security controls on client devices. This is a good option for many organizations that don't have staff specialized in those operations.

Security engineers with an MSSP are experienced in these areas since that is what they do for a living. For those of us working in other areas of IT, securing a network may be something we worked on at some time in the past, with someone who knew more, and at a time when we remembered more about network security.

Security is an area where the idea of division of labor makes a lot of sense. The idea here is that rather than trying to be good at many different things, we are all better off if we each focus on different areas and develop our expertise in those areas.

This approach to security is good for as far as it goes. The problem is that it does not go far. The MSSP approach provides an entry level of security protection. The problem is that MSSPs focus on performing a limited set of tasks and that leaves organizations vulnerable to unaddressed security needs.

## Limited scope

One of the issues with MSSPs is that they have a limited view of the security landscape and a limited set of responses to incidents.

Imagine your company has contracted with an MSSP to provide security services. The contract specifies the kinds of services the MSSP will provide and that might include configuring firewalls, running vulnerability scans, and validating policies for your virtual private network.

These are all important, and it is a significant contribution to your overall security posture to have these tasks taken care of. Unfortunately, they are not nearly the scope of what you need to mitigate the risk of attacks from determined, capable, and adaptive malicious actors. You have contracted to take care of the tip of the iceberg without addressing the risks that lie under the waterline.

What if you expand the scope of your contract and add in monitoring and alerting? Surely this is the key to protecting your assets. If someone tries to compromise your systems, you'll detect some indication of that. Right? Not exactly.

First of all, attackers are aware of monitoring and logging capabilities. Sophisticated attackers will employ countermeasures to avoid detection.

For example, an attacker who wants to steal a large data set could risk detection if the attacker tried to exfiltrate the entire data set at one time by writing it to one target device. A large data download in the middle of the night might be unusual for your systems and that kind of anomaly could trigger an alert.

A better option, from the attacker's perspective, is to download small amounts of data at one time, at random intervals, and while writing to several different target devices. This kind of approach may well leave signals that blend in with normal activity on your network and don't look suspicious at all, at least when looking only at levels of network traffic.

Another problem with monitoring is that it is easy to become overwhelmed with monitoring data. As the number of applications, services, devices, and users increase, there is more to monitor.

WARNING

Simply collecting monitoring data can't address the problem of limited visibility. In some cases, it can make visibility into the state of security in your systems more difficult to assess because you are overwhelmed with data.

REMEMBER

While MSSPs can increase an organization's overall monitoring capabilities, the scope is often limited and attackers will take advantage of this shortcoming.

## Undetected activity

Being overwhelmed with data doesn't mean you're collecting the right data and simply missing the important pieces; it can also mean you're collecting too much of some kinds of data and not enough of other kinds of data. The problem with MSSPs that have limited scope is that they have limited insight into undetected activity.

WARNING

Sophisticated attackers don't broadcast their presence or leave an obvious trail of breadcrumbs for you to follow. They use multiple methods to probe your systems, collect information about infrastructure configuration, and learn users' patterns of activity, all while leaving as little indication of their activity as possible. This is why breadth of observation is so important.

Undetected activity is like missing puzzle pieces. You may know something is happening and you may have signals, like alerts that show you some pieces of the puzzle, but you don't have enough pieces to see the full picture.

The challenge for the MSSP approach to security is that without all the puzzle pieces, MSSP can't provide you with a full picture of your security status. Additionally, MSSPs often don't provide threat hunting and analysis services to help proactively parse threat data and look for potential weak points.

TIP

Monitoring, detection, and response capabilities are all connected. Weakness in one area significantly impacts the overall strength of a security infrastructure.

The combination of entry-level security processes, limited scope of observation of relevant activities in your infrastructure, and the pretense of undetected activity puts an upper bound on the security that an MSSP can provide.

# Security and Information Event Management: SIEM

The limitations of MSSPs are somewhat addressed by a combination of security information management (SIM) and security event management (SEM) in products known as SIEM (pronounced

"sim") platforms. A defining characteristic of SIEM platforms is that they collect data from multiple other security systems. This provides additional visibility, but SIEMs still provide limited analysis and can produce large volumes of alerts that further limit really understanding what is happening in your systems.

## Broad visibility

One of the limitations of MSSPs is the limited scope of what they manage and observe. SIEMs address that limitation by collecting relevant data from a variety of sources.

It is typical for SIEM systems to deploy agents to devices for collecting and forwarding relevant data to a centralized management and analysis system. For example, a SIEM system may have agents on end-user laptops, servers in the data center, firewalls used across the organization, and other security systems, like anti-malware applications.


Some SIEM systems may employ machine learning (ML) or other forms of artificial intelligence (AI) to help filter and aggregate raw data into more useful pieces of information. This can help reduce information overload, but unless the ML models are kept up to date with the latest attack patterns and with changes in the standard operations of your organization, the quality of analysis can degrade.

When thinking about broad visibility, it usually implies visibility into your infrastructure and services. This is certainly a core facet of broad visibility, but there is more to that concept. SIEMs should have visibility into the changing threat landscape.

As new vulnerabilities in commonly used software are detected, a SIEM should be able to take advantage of those findings. It should also be configured to detect new attack patterns that may emerge as attackers craft new responses to your improving security controls.

The benefits of broad visibility are that it provides event and log data from a variety of systems and an awareness of vulnerabilities and threats. The combination of those two things should be the key to identifying signals of an attack on your systems. The problem is that data alone is not enough and you need to have mechanisms, both human and machine, to analyze and reason about that data.

## Limited analysis

SIEMs depend heavily on machine-level analysis of data. This is definitely needed to collect, filter, and analyze large volumes of highly varied data. Machines are excellent at finding correlations and detecting statistical anomalies. They aren't so great at outwitting a smart, creative, and determined attacker.

While using AI is an effective tool for detecting signs of attacks, the most common AI technique employed is ML. ML has made impressive gains in the past decade and has been applied to a wide range of challenging problems, from analyzing medical images to understanding languages.

The most effective ML models, which is what ML folks like to call the programs that get created after jamming a truckload of data through an ML algorithm, depend on large amounts of data and some serious computing horsepower. In other words, it's not trivial to come up with a good ML model, and if the model is applied to an area that is changing, like the cybersecurity landscape, you're going to be retraining models frequently.

REMEMBER

The analysis limitations of SIEMs aren't dictated by the tool itself but by the humans managing the tool. Security experts are a must when hoping to leverage a SIEM solution.

REMEMBER

It's great to have and use ML and other AI techniques, but the kinds of analysis that are available now from AI need to be complemented with human intelligence to analyze new attack patterns designed by clever attackers who know somewhere an AI tool is watching them.

## Alert fatigue

One of the best features of SIEMs is that it collects data from multiple sources. This is also the SIEM's Achilles' heel. The problem is that with so much data, it is easy to find instances of apparent problems that will trigger alerts. And that leads to alert fatigue and false positives, overwhelming engineers and analysts with alerts that are not relevant, informative, or otherwise helpful.

Imagine you have an alert that will get triggered once every 100,000 times you check a metric. Now imagine you check the metric 10 million times. That means you'll have triggered the alert 100 times. In an ideal world, those 100 alert notifications

would all be about real issues that need to be addressed. In reality, a simple metric threshold is rarely sufficient to identify an issue.

To account for this, we can make our rules more robust. For example, instead of triggering an alert if one metric is over a threshold, let's add a check on a second metric. The thinking here is that if both metrics exceed a threshold, then the chance that a real problem exists increases. We can keep adding conditions to our rules until we eliminate false positives. Excellent, we have a plan.

Now before we start crafting finely tuned alert conditions, we should remember how difficult it is to craft alert rules that trigger only on the true conditions we want to trigger on and never trigger under other conditions. We may need to try multiple iterations of condition combinations to find one that works reasonably well. And then we have to repeat that process for all alert conditions. That's just not a practical strategy. We need better options for avoiding alert fatigue, increasing analysis capabilities, and widening the scope of threat detection operations.

# Managed Detection and Response

Managed detection and response (MDR) is a security service that has emerged to address the shortcomings of other kinds of security solutions. You can find more details on MDR in the next chapter, but here's a look at three key distinguishing features of MDR.

## Easy to integrate security silos

Like SIEMs, MDRs are designed to capture, integrate, and analyze data from multiple sources. Integrating data from multiple systems can be challenging and error-prone. It definitely helps to have someone on your team who has been down the data integration road before when it comes to integrating security silos.

MDR service providers have that kind of experience. You'll probably find that your MDR of choice has already worked on similar, if not the same, security systems you use. They've seen the parts that work well in the integration process and the parts that are a little more incalcitrant.

TIP

There is no need to reinvent the wheel or learn how to integrate an array of security tools when you have experienced partners in MDR to help.

## Full scope analysis

MDR builds on the ML and statistical analysis techniques commonly used in SIEM by expanding the scope of analysis to networks, endpoints, logs, and even cloud environments. MDR brings full scope analysis to security analytics.

The capability to do full scope analysis is enabled by the amount and variety of data available, the use of best-of-breed tech tools and ML, and the presence of humans in the loop. Because MDR services are staffed with security professionals, the people on the provider end can tell which kind of monitoring tools need to look where, how to interpret the monitoring data, and how to gain valuable security insights through advanced analytical techniques.

REMEMBER

Good security analysis needs both experienced security staff and advanced tools, like ML.

## A human in the loop

If your systems are under attack, there is a human somewhere directing and orchestrating that attack. Almost certainly attackers are using tech tools to probe for vulnerabilities, mask their processes running on your systems, and stealthily exfiltrate data from your data stores.

You need a human on the other side to defend your assets. Tools can help sift through huge volumes of data, lock down servers, and block specific kinds of network traffic. AIs can help sometimes to identify the most appropriate response, but a human in the loop is the best way to detect novel attack patterns and respond to unexpected actions by attackers.

IN THIS CHAPTER

- The main advantages of MDR
- Details on what MDR services offer
- What to look for when shopping for an MDR

# Chapter 5
# MDR Deep Dive: What It Offers and What to Look For

The security solution market is vast, but even within product types, there can be a lot of variation between solutions. Managed detection and response (MDR) is no different. This chapter discusses the advantages modern MDR services aim to provide, what you can expect when investing in MDR, and some specific features to look for to help choose the service that's right for your organization.

## MDR Advantages

This section explains the primary advantages of adopting an MDR service over other security solutions discussed in previous chapters. The short version of this discussion is that MDR is a flexible solution that provides access to security expertise at a fraction of the cost of building an in-house SecOps team and equipping them with cutting-edge tools.

## Customizability

MDR service flexibility can be split into two categories: customizability and capacity for integration with a client's existing security tools. Customizability covers the capability of an MDR service to adapt to an organization's specific industry and operational needs, including compliance requirements, internal business and security policies, and any future changes to these needs.

MDR clients are not monolithic. They have different industry-specific compliance requirements, varying numbers of in-house security and IT staff, different business policy requirements, and so on. Even within a single industry, there's variation in different organizations' security service needs. For instance, in the healthcare sector, a large clinic may have no IT security staff, a few basic security monitoring tools, and that's it. A different healthcare organization may run patient sample analyses, be a large organization with a few existing security staff, and have a small suite of security tools. These two organizations may have similar compliance requirements but vastly different security service needs.


TIP

MDRs can deliver flexible services by providing the expertise and tools needed to adapt to organization-specific requirements. Security solutions can't be a one-size-fits-all offering, and this kind of customizability can only be offered by seasoned security pros with knowledge of many industry requirements and the work experience to back it up.

## Open integration

The second part of MDR flexibility — open integration — is about how the service works with any existing security tools that are already part of an organization's security infrastructure. Many will invest in an MDR to supplement their existing tools, and integration with security solutions already in place is important for retaining value in prior purchases. For instance, SIEMs are commonly used security solutions that are often already in place when an organization adopts an MDR service.


REMEMBER

Security information and event management (SIEM) solutions alert organizations of specific activity and log the events. They represent a first step into the world of security solutions but almost always require supplemental tools and a lot of management to fully leverage. MDR services can manage and analyze these logs to provide security intelligence insights, prepare

organizations for security event audits, and help comply with industry-specific compliance requirements.

The advantage of this kind of flexibility is simple: MDRs don't cause more security tool adoption headaches and don't require organizations to throw previous investments in the trash. MDR services take an "if it ain't broke, don't fix it" stance. The security tools themselves aren't the problem, it's building and maintaining the security infrastructure to fully utilize them.

## Cost

Another boon provided by MDR services is the cost advantage. The total cost of ownership (TCO) of MDR services is much lower than the alternative of hiring a full security staff and providing them with a suite of security tools. Not only are the tools expensive, but finding, hiring, and retaining a complete security team is more difficult than ever.

One of the reasons the cost of hiring security pros is so high is because of the global security staff shortage. With cyberthreats on the rise, the demand for IT security personnel has also been driven up. The number of trained, experienced professionals just can't keep up with this demand, and even if an organization manages to hire a security team, staff retention is a big problem.

Because of the shortage, security pros can ask top dollar for their expertise and many midlevel organizations can't support the cost. Even hiring for entry-level security positions often leads to employee turnover, with the new hires getting some experience under their belts before moving on to higher-paying jobs.

So where do the security professionals go? Well, some of them go to MDR service providers. MDRs are run by businesses specializing in security solutions, meaning there is no shortage of security talent. Additionally, because MDRs provide a variety of security-related services, there isn't a need to invest in as many tools to achieve proper security coverage.

## Security expertise

This book has stressed again and again the importance of security expertise, so it shouldn't be a surprise that it ends up on the list of MDR advantages. Like any industry, IT security's foundation is people. The other advantages on this list (customizability, open

integration, cost savings) are all made possible by the security experts operating the MDR service.

The advantage of security expertise is a lot more than just a knowledgeable professional available to help manage security infrastructure. The advantage of human expertise includes:

- Security strategy and policy management
- Threat intelligence and insight
- The availability of a human on the other end of the line

Security strategy and policy development are complex. It involves overlapping business and compliance needs, staff availability, cost concerns, and more. MDR services are staffed by people with experience developing strategies and policies around these restrictions, so security operations are effective at defending an organization's assets, while also not getting in the way of daily business operations.

Threat intelligence is a broad subject, but a crucial part of it is the capability to evolve defensive strategies and deployments. This kind of decision making requires a human on the job, and MDR service staff members are experienced in solving problems and shifting strategies based on the latest information. MDRs are observing and learning from many organizations, not just one. As such, the security staff has a broad view of the security landscape. A new vulnerability might be detected in one client's system and this information can be applied to other organizations.

One of the reasons security professionals at MDR service providers are so valuable is that they're constantly learning with insights for your organization as well as those from their many other clients. They can then take those learnings and improve on the support for your security operations. More than that, some MDR service providers also utilize machine learning (ML) and other advanced artificial intelligence (AI)-supported analysis techniques to interpret and respond to security information. The human element, though, is still critical to even this aspect. ML in a vacuum is useless. It requires an expert at the beginning and end of the algorithm to fully leverage it.

The last aspect of the expertise advantage is simply having access to humans for advice, not dashboards, ticketing systems, or technical documentation. Security staff members aren't the

only people who deal with security problems. Managers, system administrators, and others will have security concerns and questions, but many of these people won't have the knowledge to navigate security tool dashboards or understand technical documentation. Being able to speak with a person to help walk you through security concerns is a huge help, and MDR provides it.

# What to Look for in MDR

The advantages covered in the previous section are, for the most part, shared between MDR service providers. However, there are some key aspects to look out for when choosing a modern MDR. The biggest problem tends to be that many services will say they offer certain capabilities, such as "incident analysis," but the fine print paints a picture of what they mean when they say that.

For instance, two MDR providers may offer incident analysis, but one has access to ML analysis techniques while the other's offering is more rudimentary. Analysis overlaps with other aspects of an MDR service as well. What is the availability of support staff? What kind of policy development assistance is offered considering new threat information?


TIP

Fine details like this end up mattering a lot. They are the kind of considerations that can be the difference between an attack getting through and one being stopped in its tracks. Now, let's consider some of the biggest capabilities to look for when choosing an MDR service.

## Comprehensive logging and reporting

A lot of organizations begin their security journey with SIEM solutions to meet logging and alerting needs. This is also one of the first things to look at when considering MDR options. The "comprehensive" part of this consideration is about how the MDR service handles logs and alerts from your systems and how it deals with reporting for both internal and compliance purposes.

Incident logs and alerts can pile up fast, and the best MDR providers will be able to properly handle the deluge of information. This is part of the web of visibility that's so crucial to an effective security infrastructure. Experts should be the ones parsing and learning from logs, in addition to organizing logs to comply with industry or state regulations in case of security audits down the line.

REMEMBER

Organizations in heavily regulated industries aren't the only ones that need comprehensive logging and reporting. Any organization can benefit from the boons to threat intelligence provided by great log handling.

Security incident reporting is also important for compliance. Complete incident reporting requires knowledge of the intertwined systems that generate the information making up the meat of the document. It's a lot, and a good MDR service provider will help clients to build reports. This lifts a large portion of the reporting burden off the client and hands it to security pros with lots of experience building reports.

## Detection

An MDR service that has good detection capabilities is one that has fine-grained visibility into a client's systems and resources. This means packet-level views of network traffic, the capability to detect data exfiltration from cloud environments, and a full view of endpoint devices.

Cloud visibility is one of the most important things to look for in a modern MDR service. This is frequently a blind spot for organizations, either due to a lack of comprehensive security tools and services or simply misunderstanding the security needs of a cloud platform. Best-in-class MDR services will have a view of the cloud and be able to leverage modern threat-detection techniques, like ML and AI-driven analysis.

WARNING

When it comes to MDR detection capabilities, one red flag is the word "focus." It's a positive-sounding word, but when applied to IT infrastructure visibility, it suggests the service is lacking in certain areas. A service that focuses on endpoint detection may have a network visibility weakness, and so on. The right MDR service is the one with a broad and deep view of internal systems and resources.

The key to good detection is fine-grained visibility. Cloud visibility is an especially common weak point for organizations and many legacy MDR service providers.

## Response

Effective responses to attacks are driven by actionable information. Remediation is just one part of a response. A full answer to

a threat involves informed policies and advanced threat hunting capabilities. Following the comprehensive visibility of the MDR services, good response plans and actions are driven by high-quality threat data and modern analysis tools.

This information allows MDR provider security staff to formulate a response and inform the client. There may even be instances where the MDR service provider's response is just an alert report. IT staff might receive a security alert, get ready for action, and end up getting a report from the MDR provider that the alert was a false positive. While this seems like a waste of time, it would have been a much greater waste to have internal staff dealing with a false positive rather than a professional security team that can quickly identify false positives.

A solid MDR service is one with the availability to inform clients of attacks, the tools to remediate them, and the detection capabilities to back it all up. If an MDR provider seems like it lags in one of these areas, it's best to keep moving and find a new option.

TIP

The strongest MDR options expand threat hunting services by proactively looking for threats, not just reacting to them.

## Full integration

MDR adopters are a diverse group of organizations. From small operations with no security staff on hand to larger organizations with security teams and tools already in place, MDR can be a security boon to all of them. With this diversity also comes a high integration requirement.

A business with no security staff and a basic security toolset is easy enough for MDR providers to integrate with. The service fills in the holes, runs penetration testing and risk assessments, and helps the client develop security policies.

Many organizations have some security staff working in-house, have a set of security policies in place, and have invested in more advanced security solutions, such as modern SIEMs. Integrating with this kind of organization involves fitting within strict day-to-day operations. There is already a rhythm dictating the operation of the existing security infrastructure, security tools are working (maybe they could be working better), and there are experienced security professionals working to defend internal systems.

A strong MDR option is one that fits with an organization's specific needs, and this should include getting the MDR up and running in the first place. Organizations don't just want to keep their existing security solution investments; they want to keep their investments in people and processes.

WARNING

Look out for MDR services that only advertise integration with existing tools. A provider that emphasizes tools and not the people behind them isn't a good option.

An MDR's integration capabilities are part of the overall flexibility of the service. Integration shouldn't just be about playing nice with existing tools or fitting properly within your IT infrastructure. It should also be about fitting with the people and policies of a client's organization.

## Incident analysis and forensics

Threat incident analysis and forensics is the process of understanding and learning from cyberattacks and attacker behavior. Incident analysis doesn't just occur after a successful breach. Even blocked attacks should be analyzed for valuable information about future threats.

Because MDRs are always on, client organization staff may wake up to a security alert that has already been analyzed by the provider's security teams and found to be benign or already dealt with. What sets modern MDR solutions apart from less capable ones is more than just availability, though. A big part of it is how MDR services perform the analyses and forensic operations on threat data.

A good MDR provider is one that evolves with the security landscape, and this includes evolving its own internal procedures and tool sets to meet modern threats. There are new analysis and threat forensic technologies and techniques developed every year, with ML and AI-supported processes currently on the cutting edge.

ML-driven analysis helps security professionals see things even they might miss when investigating a threat. The sophistication of current attacks can hide behavior and infiltration points, exfiltrated data, and more. Advanced analysis tools should be a part of any MDR service an organization seriously considers using.

This key aspect of an MDR service is difficult to find. There are many MDR solutions that offer incident response plans, but the combination of response and forensic services is both crucial to a strong security posture and a rare thing in the MDR world.


TIP

Detailed forensic reports are an important part of any security infrastructure. A good MDR service should provide open communication about security incidents and the follow-up analysis.

## Human expertise and availability

One of the main draws of any MDR service is the human element. A full-featured security operations service is a huge cost saver. It lightens the managerial and operational load of hiring and maintaining security teams and tools, and the flexibility it provides helps organizations respond to the current threat landscape.


TIP

Be aware that expertise and availability can differ between services. The first question to ask about an MDR provider: "Is this an established IT security provider with experience dealing with modern threats?" There is a large demand for security tools and services right now, so there are new security vendors popping up every year. Some of these will become reputable, seasoned security companies in a few years, but now is not the time to take a chance on vendors just entering the industry.

Similarly, vendors of legacy security solutions, such as managed security service providers (MSSPs), are now trying to reposition their products as modern options. Unfortunately, an MSSP with a fresh coat of paint is not a comprehensive MDR service. The human availability at providers like these will not be as strong as with a modern MDR. Communication will be limited, provider-side security pros won't have access to the latest analysis and detection tools, and the security services they provide may not even line up with the basic advantages of MDR in general.

The right MDR provider for your organization will be staffed with seasoned security professionals equipped with the best tools and have true 24/7 availability. People are what make MDR services stand out the most in the crowded security solutions market, so assessing the quality and availability of their expertise should be a top priority.


REMEMBER

True 24/7 availability might mean getting urgent security alerts at 3 a.m., but this is better than the alternative.

Its service is built on the belief that humans are the most important element of any comprehensive security service, these services should have high integration capabilities, and that the end goal should be a holistic view of an organization's attack surface.

## Humans are the key

Just as humans are the driving force behind today's security threats, they're the force behind the best security solutions for combating those threats. We take a humans-first approach to MDR by integrating human intervention and problem solving into almost every step of the threat response lifecycle.

REMEMBER

A truly successful MDR service must combine the intelligence and creativity of human minds with powerful security technology. An example of this philosophy in action is the thousands of alerts that SIEMs can produce every day. Security experts are needed to sift through them so alert fatigue and false negatives don't impact security operations.

These security pros should also be easily accessible to clients. And it's not always just about alerts. Accessibility to analysts for questions and updates is important because two-way conversations and real relationships build a strong cybersecurity program. People on the client side of the equation are also vital to maintaining a secure program, so they provide 24/7 service from security operation centers all within the United States.

## Don't replace existing tools

Some organizations may be enlisting the help of an MDR service to help build their security operations from the ground up, but many clients already have tools and staff in place. ensuring easy and open integration with existing tools and policies is an important part of client success.

Organizations with previous security investments shouldn't have to throw out tools and processes to bolster their security infra-structure.

# Chapter 7
# Ten Things to Remember about MDR

This chapter is an overview of the ideas discussed in this book. It covers security challenges organizations currently face, capabilities to look for when shopping for a managed detection and response (MDR) service how MDR services set themselves apart from other security solutions, and more.

## The Security Landscape Is Evolving

Cyberattackers, the infiltration techniques they use, solutions available to defend against them, and daily business practices are all rapidly changing. The push to work from home, as well as new ways to get paid for cybercrime, are contributing to a rising interest in accessing private IT systems. With more endpoints to cover than ever, the attack surface is rapidly expanding, and attackers are always developing new strategies to circumvent existing security measures. This means organizations need flexible and adaptable security solutions to secure their internal resources.

## Modern Attacks Can Be Hard to Identify

Although there are still tried and true attack techniques floating around, many bad actors are developing sophisticated, new infiltration strategies. Organizations are also utilizing new tools, such as cloud platforms, to supplement and bolster operations. These new systems can be big blind spots for organizations, and attackers know it.

## There's a Visibility Problem

In addition to security blind spots, many organizations don't have the capability to monitor all their attack points with the detail that the modern security landscape requires. Fine-grained visibility of network, endpoint, log, and cloud resources is needed for proper threat detection given the sophistication of today's attacks.

## MSSP, SIEM, and MDR Bring Different Things to the Table

Many organizations already have SIEM solutions in place for logging and alerting purposes. These tools are a blessing and a curse. While the sheer amount of information is great for compliance-heavy industries and collecting data on attacks, most organizations can't deal with the flood of alerts that SIEMs can provide.

REMEMBER

Managed security service providers (MSSPs), often a next step, offer some aid with this but often don't provide the comprehensive detection and response capabilities required to deal with modern threats. MDR, on the other hand, combines (and furthers) the visibility provided by SIEMs and aids clients in managing security infrastructures and responding to threats.

## MDR Accelerates the Incident Response Lifecycle

MDR services provide a lot to clients. All the tools and techniques are helmed by security professionals, meaning whenever a security event occurs, there is a qualified person to respond to it. The time to detect, isolate, remediate, and analyze a threat makes a big difference when each packet of stolen data could cause severe impact to users and customers or the organization itself. The incident response lifecycle should be as thorough and fast as possible, and MDR services have the capability to significantly reduce dwell time.

## Not All MDRs Are Created Equal

While there are plenty of similarities between MDR services, the fine print can matter. One MDR may specialize in monitoring and analyzing network-related threats, while another focuses on endpoint detection and response. Both services are incomplete in today's security landscape. The best MDR is a modern one with a complete tool set and experts available to leverage it.

## Human Expertise

The security personnel shortage continues, and by some metrics, it's worse than ever. This means security talent is hard to come by and expensive to retain. Unfortunately, security solutions are just tools and can't do the work of defending your systems for you. People are still the backbone of IT security, and access to human expertise is vital to a comprehensive security infrastructure.

## MDR Is Always on and Available

One of the primary advantages of MDR services is their wide availability. Even when the office is empty, MDR providers can monitor client systems 24/7 and react to threats as they are detected.

## MDR Complements Existing Security Tools

Some MDR solutions allow for relatively painless, open integration with existing tools. For instance, MDR clients will often already have SIEM solutions. These can be complemented by the detection, response, and analytics capabilities brought by MDR services. MDR's flexibility with existing systems saves organizations money and time by getting a security infrastructure up and running using what's already in place.

## MDR Can Evolve with the Landscape

With teams of security professionals on staff, MDR services can react to the shifting security landscape. The experts at MDR providers will be up to date on the most recent security trends, infiltration strategies, and analysis techniques. MDR isn't just flexible in how it complements organization-specific needs but also in how it can react to changing security environment conditions.