# 3 Components to Consider When Selecting an MDR Service

TechTarget

**In this handbook:**



# 3 Components to Consider When Selecting an MDR Service

*DANIEL CLAYTON*

As cybersecurity threats grow, security teams across the world are struggling to keep pace. An average security operations center receives more than 10,000 alerts daily. This number can be so overwhelming that many SOC teams triage less than half the alerts they receive.

Most SOC teams also lack the time or expertise to conduct a full incident analysis, which leads to poor responses and ineffective recovery. Due to these challenges, many organizations are turning to managed detection and response (MDR) services to help them hunt, mitigate and contain cyberthreats.

## THE IMPORTANCE OF MDR

MDR is a new and fast-growing service within the cybersecurity industry. The MDR service market is expected to reach $2.2 billion by 2025. According to Gartner, 50% of organizations will use MDR services by the same year. This rapid growth is due to MDR's ability to address the most urgent challenge facing cybersecurity teams in organizations of all sizes, across all industries: It's not a question of *if* you will be breached, but *when*.

Security teams must assume their networks have been compromised; reactive detection capabilities alone won't protect an organization. A proactive plan ensures, once a security team identifies a problem, there is a quick, effective response.

Adversaries operate around the clock, and there is no way to predict when an attack will happen. So, organizations should have 24/7 security operations. However, this is resource-intensive, and many companies don't have the in-house capabilities.

These reasons are why companies turn to MDR services.

## DEFINING MDR SERVICES

Many different definitions of MDR exist in the industry. Forrester Research defined MDR as the "application of advanced analytical techniques, proactive threat hunting and automated response, based on escalation workflows predefined by a managed security services provider."

MDR services are delivered in a variety of ways, though the industry seems to agree on the following elements as the most basic deliverables of an MDR service:

- proactive response
- cyberthreat hunting

- 24/7 operations

A significant gray area remains, however. Buzzwords and jargon have always existed in cybersecurity, with new technologies constantly hitting the market in response to the ever-changing threat landscape. In some ways, buzzwords are unavoidable. Those who have worked in the industry for years may roll their eyes at the ubiquitous claims of AI or the latest flux capacitor solving all our challenges.

MDR may seem like the latest example. Yet, the lack of standardization with regards to terms, processes and technologies makes it difficult for organizations to assess and select vendors' services, tools or technologies. In addition, these services often turn into alert factories that further overwhelm security teams and provide little value, leaving CISOs dissatisfied with their investments and the organization no better protected than before.

It's time to agree upon industry-wide standards for what constitutes a threat hunt and response, what metrics should be reported to customers, and other key measurements when it comes to MDR services.

When assessing MDR providers, it is important to evaluate their services in three key areas: response, threat hunting and 24/7 service.

Look for these capabilities when assessing potential providers.

## Response

MDR services are presented as a team of expert security analysts "keeping an eye" on your organization 24/7. They promise to help protect your data with a mature and comprehensive security plan that can detect and respond to attacks -- even those evading controls already in place.

This sounds great, but it's important to understand what providers mean by *response*. Far too many providers notify their clients of an incident and leave the customer to deal with the attack. Important questions to ask MDR providers include the following:

- What proactive response capability do you have?
- To what extent are those response actions automated?
- What is the role of the customer in response actions?
- What is the approval process for response actions?

## Threat hunting

Cyberthreat hunting is a critical component of MDR services. When performed properly, it requires high levels of expertise and relevant and contextualized threat intelligence. Threat hunting should incorporate a contextualized view of likely bad actors and their associated tactics, techniques and procedures, as well as a clear understanding of the business and IT environment being defended.

When evaluating MDR providers, ask them:

- How do you define a threat hunt?
- How is a threat hunt measured?
- What performance indicators will you provide?
- To what extent are threat hunts automated?
- How is threat intelligence incorporated into the threat hunting program?
- What are the goals and outputs of the threat hunting program?
- What are triggers for threat hunts?

## 24/7 operations

At first glance, it may appear easy to evaluate whether an MDR service provides 24/7 operations, but even this standard can vary. By asking the right questions, an organization can get a thorough understanding of the operating model, the staffing levels and the location of the analysts tasked with protecting your data.

Ask an MDR provider about the following:

- out-of-hours callout processes
- staffing levels during out of hours
- follow-the-sun shifting

Also, ask whether they provide a remote, co-sourced SOC or geoindependent SOC -- meaning, ask if they have a team of analysts working remotely that serves a single customer base or multiple SOCs in international regions serving customers from the same region. MDR services provide a critical capability to organizations lacking the expertise or resources to build an operation themselves or those that want to focus their efforts on other areas. MDR serves as a safety net when other security controls fail and provides an ongoing view of an organization's environment and its individual threat landscape, as well as how both are evolving at any time.

The critical nature of MDR outcomes makes the selection process critical. In the absence of industry standards, the responsibility is on companies to ask the right questions when evaluating potential partners. To make an informed decision, companies can't simply view these critical components as checkboxes. Ask the questions, kick the tires and make the right decision.

## About the author

*Daniel Clayton is vice president of global security services and support at Bitdefender. His responsibilities include managing customer security environments from the company's SOC. Clayton has more than 30 years of technical operations experience and has led security teams for the National Security Agency and British intelligence.*