Ontinue

eBOOK

5 Signs MDR Is Right for Your Organization

Introduction

Today's CISOs face the ever-growing challenges of maintaining security operations, including detection and response capabilities. For most organizations, it's simply too time-consuming and costly to spin up an internal security operations center (SOC) to detect and respond to security incidents efficiently and effectively. Many CISOs choose to partner with managed detection and response (MDR) and MDR service providers. MDR service providers extend protection to both endpoints and networks, and can also provide coverage for internet of things (IoT) devices or operational technology (OT) networks.

Finding the right MDR/MDR partner to enable effective security operations and mitigate risk can quickly deliver a strong return on investment (ROI) and better security outcomes across the entire security lifecycle: not only strengthening detection and response capabilities but providing insightful assessment and helping to proactively harden and mature your security program.

If you're wondering whether an MDR solution could help your organization, consider whether these five signs sound familiar:

1 Alert Fatigue

Each day, a SOC can easily receive hundreds of millions of raw events from countless telemetry sources. Consequently, perpetually resource-constrained teams spend time researching this onslaught of alerts and dealing with emergency issues rather than focusing on strategy and process improvements. When security teams are overwhelmed with alerts, it not only creates immediate security issues if critical alerts slip by without proper investigation, but it also can create a vicious cycle of employee burnout and high staff turnover, exacerbating the problem.

A modern security information and event management (SIEM) platform, such as Microsoft Sentinel, aggregates events and leverages machine learning and automated playbooks to aggregate and correlate the raw events down to a more manageable number of alerts—but that's only part of the solution. Partnering with an MDR service provider empowers your SecOps team by eliminating daily firefighting, freeing the team to focus on strategic security initiatives that deliver value to your organization.

Better yet, an MDR service provider will use machine learning and automation to resolve the majority of alerts, freeing human analysis within the SOC to act on alerts requiring more expertise to resolve. Technology that allows those experts to focus on what delivers the most value results in leaving only the most critical alerts—the ones that really matter—for your internal SecOps and IT teams to address.

Importantly, a modern MDR provider should use technologies like Microsoft Teams to collaborate with your internal teams to ensure these alerts are understood in context and properly addressed. While the graphic below highlights the importance of collaboration, within the context of alerts, instant communication and the ability to truly work together can be critical. Ticketing through a portal can be a useful way to track records for audits, but modern cybersecurity requires the ability for multiple teams within an organization to coordinate with their MDR partner in real time.

2 Tool Sprawl

Security professionals employ myriad tools in their pursuit of effective cybersecurity. The 2021 Cyber Resilient Organization Study by IBM Security found that 83% of organizations today use more than 20 separate security tools and technologies on their networks—and 30% use more than 50.[1]

Counterintuitively, using more tools doesn't necessarily translate into better security performance. Increasing the number of tools often creates complexity and inhibits efficiency, which negatively impacts security performance. Even basic software maintenance and management becomes nearly impossible: Simply keeping track of and managing so many different tools is too burdensome for overworked InfoSec teams.

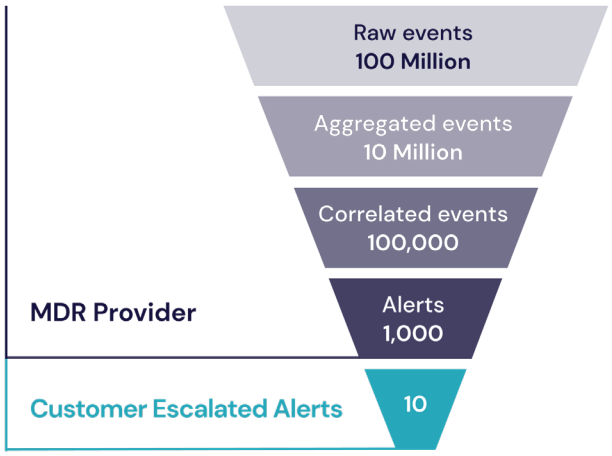

Figure 1: Your MDR/MDR provider helps your internal IT and security teams avoid alert fatigue and focus on only the most critical alerts.

According to the IBM study, organizations using more than 50 tools rank 8% lower in their ability to detect and 7% lower in their ability to respond to an attack than organizations with fewer than 50 tools[2] (see Figure 2). It appears that once the number of security tools reaches a saturation point, where the gaps in the can become bigger vulnerabilities than those the armor was protecting in the first place. The study further showed the average time to detect and contain a breach is 212 days and 75 days, for those with over 50 security tools and those with fewer, respectively.[3]

The right MDR or MDR partner will maximize your existing security investments and reduce complexity by, for example, consolidating the Microsoft security tools you already own.

While no human can effectively sort through millions of alerts, only trained humans can make the right decisions quickly enough to stop threats and limit damage. An MDR or MDXR service operated by highly skilled security experts and backed by world-class machine learning-driven anomaly detection offers the best way to improve your organization's incident response capabilities and reduce the time it takes to respond to a threat.

High Mean Time to Respond (MTTR)

Today's threats have become more sophisticated and often persist in a victim's environment for extended periods of time. These advanced persistent threats (APTs) worm their way into your network, move laterally from one system to another, wait patiently and stealthily, and then choose the most opportune time to cause maximum damage.
In the section above, we touched upon the affect tool sprawl could have on time to detect and respond. The same IBM Security research highlighted above further demonstrates the cost of slow detection and response. That study correlates the cost of a breach to mean time to detect (MTTD) and MTTR: The average cost of a breach with a lifecycle (the time from detection to containment) over 200 days is $4.87 million compared to $3.61 million for a breach with a lifecycle of less than 200 days (see Figure 3).

The more time an attacker has within your environment, the more problems they can cause for your organization. High MTTD and MTTR translate to more lost revenue, lost productivity, lost value.

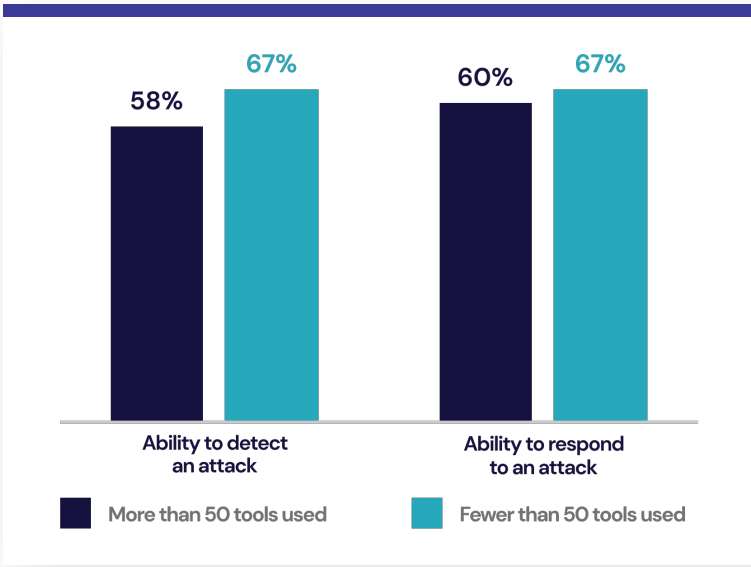

Figure 2: Deploying too many tools increases complexity and negatively impacts detection and response.

Lack of Communication Between SecOps and IT

SecOps and IT teams often have far too much to do, and not enough time to do it all. Staff often have conflicting priorities and little time to discuss issues or align activities. The situation isn't helped by the daily deluge of alerts and lack of skillsets required to manage all of the security tools an organization deploys. And too often, those myriad tools have their own portals and their own siloed workflows.

This tends to result in issues simply being "thrown over the wall"—unprioritized and with little to no context—from SecOps to IT. If they're spending most of their time on daily firefighting, SecOps teams simply don't have the time to develop playbooks that can help IT more effectively mitigate specific threats. Inevitably, this situation leads to poor or ineffective communications between these teams.

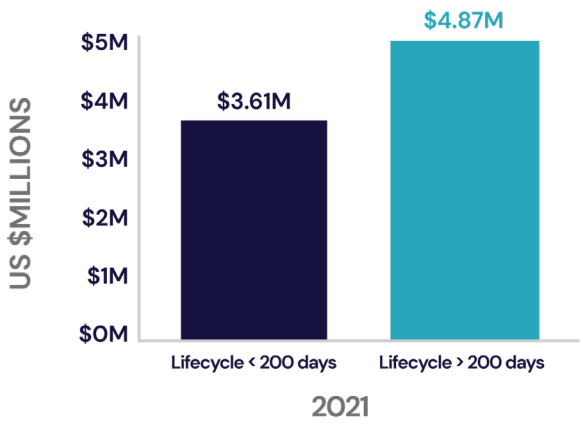

Figure 3: Average total cost of a data breach based on average lifecycle

Conversely, a modern MDR or MDR service should have the capabilities that foster collaboration not only between the provider and your organization, but between your internal teams, including SecOps and IT. For organizations using the Microsoft ecosystem, Microsoft Teams enables real-time collaboration while plugging into existing IT processes and leveraging common systems and existing investments in Microsoft technologies. Prioritizing and enabling collaboration in every aspect of the service is essential to rapidly increasing your organization's security maturity.

Inability to Measure Success and Prove Security Efficacy

The ultimate goal of security is to prevent attacks, minimize risk, and improve security posture. But it's very difficult to improve what you can't measure, and measuring success—or even progress—often presents a daunting challenge. Most CISOs today recognize that it's not if, but when an attack will succeed against your organization. To reduce risk, your MDR or MDR service provider should offer different measures of success while enabling security efficacy. Defining key performance indicators (KPIs), such as MTTD and MTTR, will help you measure the effectiveness of your security operations. Ensuring you have a current baseline for these KPIs will help you identify objective goals for continuous improvement. In addition to MTTD and MTTR, other important metrics might be less obvious, such as staff turnover and software-related costs. Both metrics should trend lower with an MDR or MDR partner that reduces alert fatigue and staff burnout while consolidating the tools in your security stack—instead of recommending their own new proprietary tools.

Defining key performance indicators (KPIs), such as MTTD and MTTR, will help you measure the effectiveness of your security operations.

Conclusion

Managing the complexity of a modern cybersecurity program in a cost-effective way has never been easy. As the threat landscape has grown more treacherous and the cybersecurity job market has become more competitive, it's only grown more difficult. Managing all aspects of a security program in-house remains a challenge, even for the largest organizations.

Partnering with the right MDR service provider can lead to immediate improvements in your security posture and continually help your organization harden security over time. This can be achieved both by freeing your security staff to focus on mission-critical tasks rather than firefighting alerts, and by providing insights into your environment's vulnerabilities and how to fix them.

References

[1] 2021 Cyber Resilient Organization Study
[2] 2021 Cyber Resilient Organization Study
[3] 2021 Cost of a Data Breach Report

Ontinue

About Ontinue ION: Nonstop SecOps

Ontinue ION is the MXDR service of choice for Microsoft security customers that want to accelerate MTTR, proactively reduce risk, and reduce costs. Together, the Ontinue ION Platform and designated cyber defense experts build a deep understanding of your organization's risk posture that focuses prevention, detection and response efforts to reduce risk and mitigate threats.

AI-driven automation delivers fast, accurate investigation and response. Our one-of-a-kind Microsoft Teams interface provides real-time access to our 24/7 ION Cyber Defense Center to resolve every incident.

As the 2022 Microsoft Security MSSP of the year, Ontinue knows how to optimize your Microsoft investments, simplifying your technology stack and improving ROI.