CRITICALSTART™

Guide to Managed Detection & Response

Deploy an MDR Platform That Can Protect Any Business

CRITICALSTART

Executive Summary

Managed Detection and Response is reinventing information security. In this paper, you will learn how it provides far better visibility into threats and enables an active, real-time response to mitigate any impact. We'll discuss what to look for in an MDR provider and—most importantly—why every alert matters.

Topics Include:

The business case for managed services

How MDR provides better protection in today's environment

The right questions to ask an MDR service provider

How to know if the MDR you're considering is really MDR

Why every alert should be treated equally

What kind of real-world results can you expect through a solid approach to MDR

CRITICALSTART

The Imperative for Managed Services

Our world is increasingly digital. Ten years ago, just under 30 percent of the population was online. In June 2020, that number stood at almost 60 percent. And as 2020 witnesses a dramatic shift to a remote workforce, the prevalence of online attacks is ever present. According to the 2020 Cost of a Data Breach Report, 76% of respondents at organizations that shifted to remote work expect that working from home could increase the time it takes to identify and contain a data breach. 70% of respondents expect remote working could increase the cost of a data breach.

But Here's the Real Challenge:

The same report found that remote work could result in costs that were nearly $137,000 higher than the global average of $3.86 million and respondents estimated that the shortage of security skills increased costs by an average of $257,000.

Contributing to this cost is the effort and expense of deploying a Security Operations Center (SOC). If an organization tries to respond to threats by building this capability internally, an internal SOC can cost a minimum of $750,000 in employee salaries alone.

Calculating the Cost of Digital Security

Need to determine the cost of security analysts to protect your infrastructure? Consider the following:

An average endpoint generates **5000** security alerts per year

\+

2000 endpoints generate **10,000,000 alerts annually**

\+

A security analyst takes an average **15-30 minutes to investigate one alert**

\+

Investigating only the alerts classified as "high" or "critical" would require **hiring 21-22 analysts**

=

An average analyst's salary is $35/hr., so those 21-22 analysts would require an investment of over **$1.5 million annually.**

For more information on calculating the cost on your own SOC, review our Total Cost of Ownership eBook.

CRITICALSTART

MDR Lifts the Security Burden

Managed Detection and Response (MDR) is where many firms are turning to protect their business and alleviate staffing and technology concerns. By working with a security partner that utilizes their own analysts, tools, threat identification strategies and procedures to be proactive in responding to cyberattacks, damage from these attacks can be effectively mitigated for far less cost than an internal solution.

First, is the Consideration of Tools

MDR often utilizes artificial intelligence (AI) to prioritize alerts, consolidating everything onto one platform to provide comprehensive visibility to the SOC. Analysts can then decide on the alerts that represent a security threat and respond with direct action, such as isolating an endpoint, changing passwords, or whatever action in necessary to prevent the attack from moving within the network.

MDR is the latest evolution to protect organizations from a highly-diverse, multifaceted threat environment, including everything from individual hackers to nation states. But perhaps its most important benefit is that a company can access the latest security expertise without hiring internally, and available resources can grow with the business without the need to add additional personnel.

For more information on calculating the cost on your own SOC, review our Total Cost of Ownership eBook.

CRITICALSTART

How to Select an MDR Partner

The essential key in selecting an MDR vendor is to realize that not all are created equal. Consider asking a potential vendor these questions as indicators of how they will perform when your organization is facing a threat:

- How long does your team take to respond to alerts? Are there contractual obligations around this?
- Will my company have access to your SOC as needed or is that an additional charge?
- Is there any hardware associated with this tool?
- If my company grows quickly can the MDR tool you're using scale quickly?
- Can this tool help me respond to both SIEM and EDR from one console?
- Can we investigate and respond to alerts natively from our phones?

Key Takeaway

The last two questions are particularly important, as they can determine what kind of control and visibility you will have in determining the direction of your new security environment. Information on alerts needs to be accessible in one platform on any device you use to do business. It should be accessible at any time and place to ensure critical threat and response information is always available as it happens.

CRITICALSTART

Qualities you might look for in an MDR Partner

Requirement	Ability to Provide?	
Contractual refunds based on missed-SLA's	Yes	No
Access to the comments, rules, audit logs, and people working on alerts	Yes	No
50% or greater employee owned business	Yes	No
Actively contributes zero day research in excess of 20+ zero days/year	Yes	No
Service provides metrics for effectiveness	Yes	No
Ability to collaborate/talk to analysts, investigate endpoints, and isolate, if required, from mobile device	Yes	No
SOAR vs SIEM based approach	Yes	No
24/7 capabilities	Yes	No
US-based SOC	Yes	No
SOC retention rate of 100% over 3+ years	Yes	No
Investigate every alert looking for known good events against a database of known good behaviour / Auto-resolves known good behaviour	Yes	No
Can leverage multiple endpoint solutions / Service is not tied to one technology manufacturer	Yes	No
A trusted-behaviour-orientated method of handling false positives (not a resource-, input-, or priority-orientated method)	Yes	No
Ability to review activity for investigated alerts that are not forwarded to client	Yes	No
Provider has positive cash flow	Yes	No
Less than 1.5% voluntary turnover on executive leadership over 3+ years	Yes	No
Cyber security is the primary business focus, not a tagential business unit	Yes	No

CRITICALSTART

Is it Really MDR?

As you're evaluating solutions, it's important to determine if what you're evaluating is a Managed Security Service Provider (MSSP) or true MDR. An MSSP takes incident and event data and monitors it 24 x 7. But an MSSP can be overly broad and does not dive deeply into the underlying causes of alerts. MDRs use their own SOC, security processes and infrastructure to really absorb alert information and uncover the hidden reasons behind them. Effective MDRs also have a much deeper and more sophisticated response plan in place to identify both vulnerabilities and threats, and then they take a dynamic response to resolving those issues.

Endpoint or SIEM?

Exactly what information should be fed into an MDR process is an interesting question. Many providers simply ingest data from Endpoint Detection and Response tools. These tools primarily search for advanced threats on endpoints, with activities such as registry monitoring, searching for modifications to file structures and validating signatures. The behavioral analysis ability of these tools also provides a capability for forensics during incident response.

But to be truly effective, MDR must process a wider depth and breadth of information. Data from Security Incident and Event Management (SIEM) tools is also essential, as it can identify, monitor, record and analyze security events in real-time. It provides a comprehensive and centralized view of the entire security scenario of an IT infrastructure. It can provide correlation to offer context on data and to create relationships based on predefined rules, architecture or alerts. It's also adaptable to different vendors, sources of information and data formats. While many companies neglect SIEM, or relegate it to log collection and compliance needs, any MDR approach must be comprehensive enough to make use of all the robust capabilities that SIEM has to offer.

CRITICALSTART

Treat Every Alert as Critical

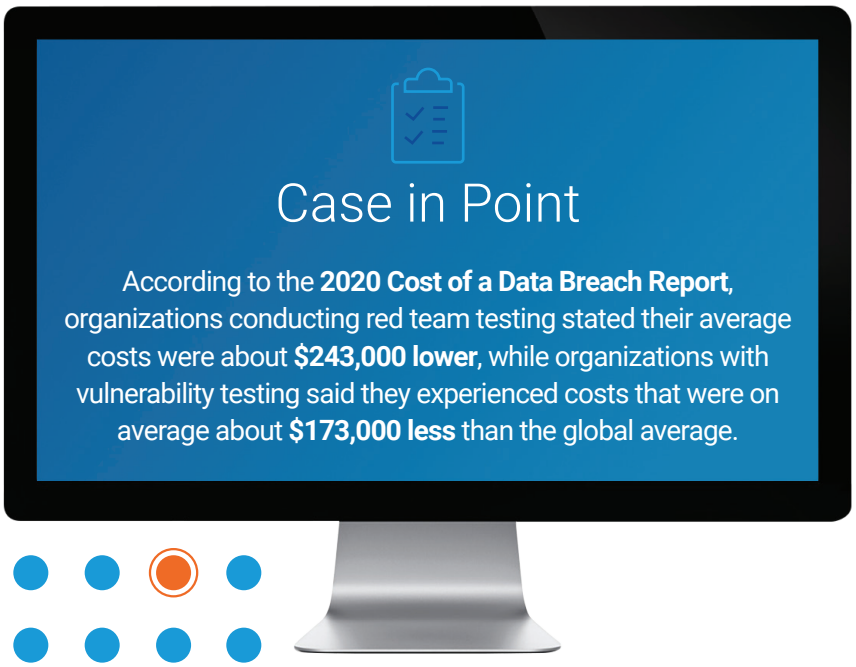
The most essential component of any successful MDR provider is that every alert collected must be treated equally. With thousands of alerts pouring in from EDR and SIEM tools, many vendors will actually disable detection logic to prevent alerts that they feel do not require attention. Others may rank alerts by categories such as critical, high, medium, low or informational, and only focus on the alerts that appear critical, (or maybe high if they have the time.)

The problem is that attackers are increasingly being detected through a SIEM platform appearing through medium, low and even informational alerts. A top-down approach to dealing with alerts is simply not sufficient in today's threat environment.

> A far more effective strategy is to use a trust-oriented approach to handling alerts at scale. An MDR vendor should work with their client to build a Trusted Behavior Registry (TBR) to determine which alerts indicate normal behavior and can be trusted. Resources can then focus on the alerts outside of this registry, regardless of how threatening they may appear at first.

Going the Extra Mile

An MDR provider should also be fluent in all vulnerability detection, threat identification and active mitigation strategies. These include intrusion detection systems (IDS) and intrusion prevention systems (IPS), threat hunting and SOC services. They must be able to analyze an environment and make recommendations on the right tools for the job. And these recommendations must not be limited to what the vendor is comfortable with, but instead focus on the needs of the client. This includes supporting implementation, optimization and monitoring to ensure that all tools work together in concert to deliver maximized efficiency and protection.



CRITICALSTART

How to Measure Success

When working with an MDR provider, if they have the right team, tools, methodology and process to protect your organization, then **over 99 percent of security alerts should be resolved effectively**.

We've also found that many companies accept dwell times, or the time from when an incident is first detected to the final resolution, of 100 days or more. With the right MDR in place, we've found that **dwell time should be 22 minutes on average**.

How CriticalSTART Achieves These Types of Results

The CRITICALSTART approach to MDR achieves results by following all of the highly-successful strategies outlined in this paper, and through an industry-first combination of the following:

Resolution of every alert

A zero-trust policy toward alerts, by building a **trusted, known-good registry**

100 percent transparency for client teams, including the industry's first MOBILESOC where you can remotely resolve and remediate endpoints, and collaborate with SOC analysts with full audit trails

Integration with industry-leading security tools including:

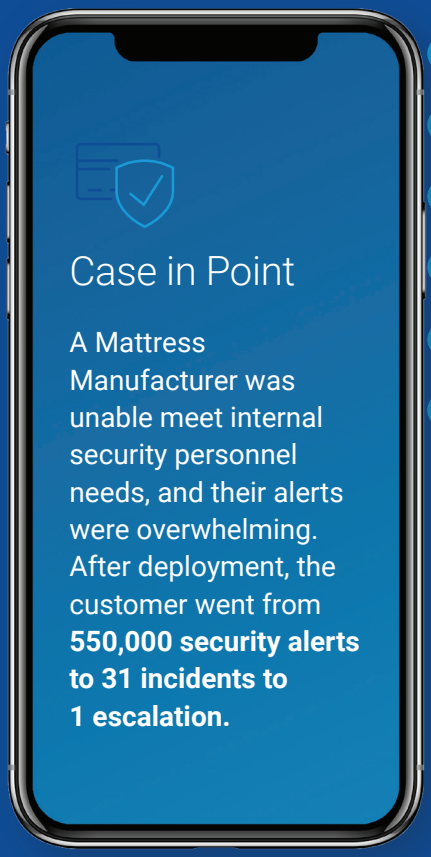
- Microsoft Defender Advanced Threat Protection
- SentinelOne
- DEVO
- CROWDSTRIKE
- splunk>
- CORTEX
- vmware Carbon Black
- BlackBerry

CRITICALSTART

CRITICAL**START** Delivers:

We support a **State Information Technology Provider** with **30,000 Endpoints through MDR** that provides a single correlated view and active response services to threats.

We enable an **International Energy Infrastructure Provider** to present a strong united cybersecurity front with the least amount of user and business obstructions through deep API Integration of their tools, **24x7x365 monitoring, and robust analytics.**



Ready to Learn More?

This overview is meant as a primer to guide your MDR decisions, but it's only the first step. Contact a CRITICAL**START** representative so we can learn about your unique security situation and how we can customize our MDR platform to help you resolve every alert and shut down any vulnerabilities your business may be facing.

To see how we can help, contact us at criticalstart.com/contact

CRITICALSTART