MDR Managed Detection & Response MANIFESTO

from the people at Alert Logic®

MANAGED DETECTION AND RESPONSE (MDR) IS AN EVOLVING FORM OF PROTECTION, BUT ALL MDR MUST FOLLOW THESE TENETS.

THE SEVEN TENETS OF MDR

1. **REDUCE** THE **LIKELIHOOD OR IMPACT** OF SUCCESSFUL ATTACKS.
2. **PROVIDE 24/7 VISIBILITY** AND **COVER ALL ASSETS** IN AN ORGANIZATION.
3. **CONTINUOUSLY BE REFRESHED** WITH RESEARCH ON NEW THREATS AND VULNERABILITIES.
4. **AUGMENT TECHNOLOGY WITH HUMAN INTELLIGENCE** TO ENSURE ACCURACY AND VALUE.
5. **PROVIDE CUSTOM RESPONSES** THAT REFLECT BUSINESS AND ATTACK CONTEXT AND CAUSE.
6. **SCALE** TO DELIVER TECHNICAL ANALYSIS AND HUMAN INSIGHTS ACROSS DYNAMIC ENVIRONMENTS.
7. **DELIVER RESULTS AND REPORTING** THAT ARE CREDIBLE, ACCESSIBLE, AND USEFUL.

Contribute to the conversation for advancing MDR: ***#MDRmanifesto***

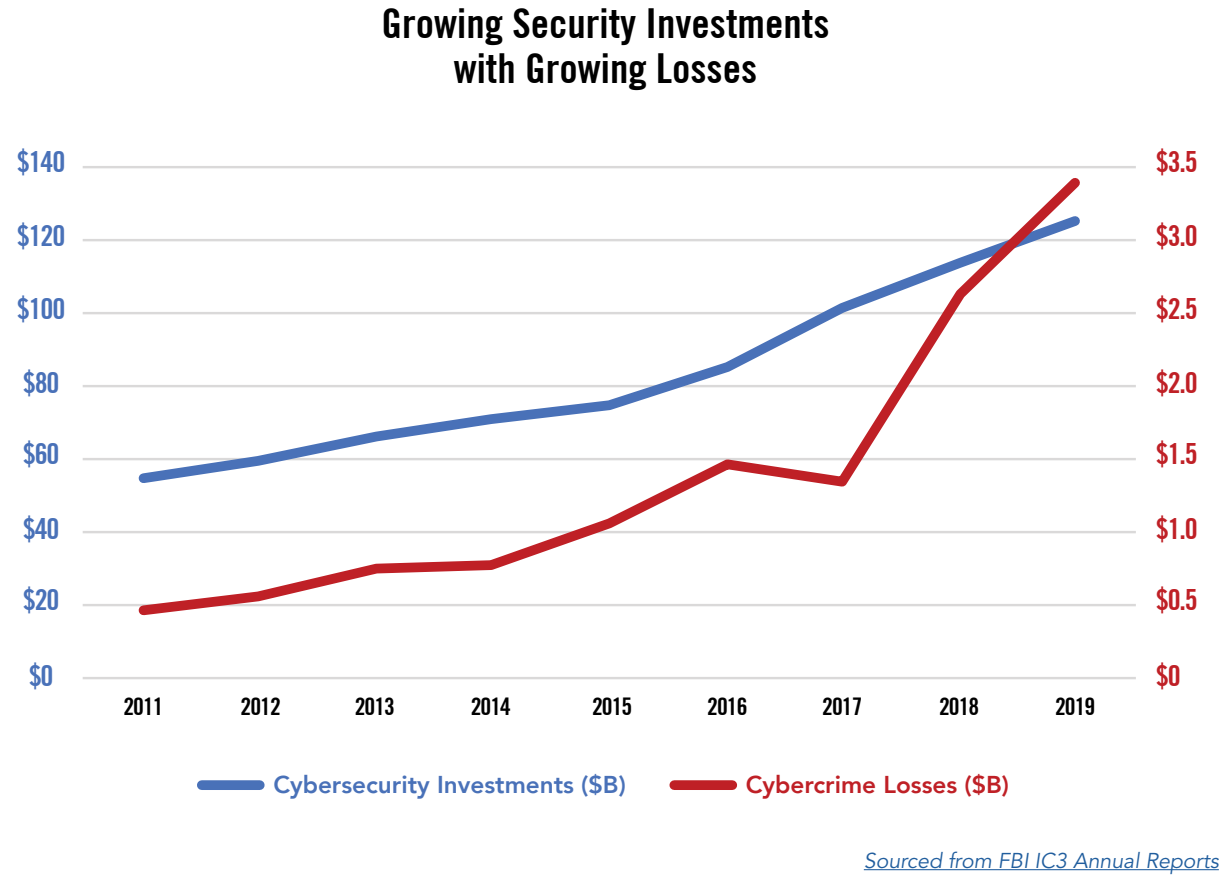
from the people at Alert Logic®

The Managed Detection and Response (MDR) Manifesto is intended to clearly define the value organizations should expect to receive when they add MDR to their security plans and budgets. In addition, this manifesto serves to clarify and standardize on the definitions and capabilities associated with MDR.

For example, a simple term like "protection" can mean anything from preventing network access, to enabling secure network access, to encrypting data, or testing the security of networks and encrypted data. The potential to provide protection against attacks and the reduction of damages from successful attacks are driving heightened interest and investment in MDR.

Nowhere are the effects of this confusion and heightened interest clearer than in the mapping of trends for security spending and security breach costs over time. According to Gartner, "end-user spending for the information security and risk management market is estimated to grow at a compound annual growth rate of 8.7% from 2018 through 2023 to reach $188.8 billion in constant currency."[1] In 2017, the total end-user spending for the information and security risk management market was $112.9 billion in constant currency.

As spending on security continues to increase, the chart below shows the costs associated with breaches also continue to rise. This paradox is directly attributable to a combination of insufficient understanding of risk and an increasingly confusing set of point solutions to the problem. This manifesto describes the virtues of MDR in clear terms, setting boundaries and expectations around the benefits and limits of the capabilities of this approach in the widening security arsenal.



Sourced from FBI IC3 Annual Reports

[1] *Gartner, Forecast: Information Security and Risk Management, Worldwide, 2017-2023, 4Q19 Update, Rustam Malik, Christian Canales, Ruggero Contu, Lawrence Pingree, Elizabeth Kim, John A. Wheeler, Mark Driver, Nat Smith, 20 December 2019*

What is MDR?

Managed detection and response solutions identify active threats across an organization and then respond to eliminate, investigate, or contain them. MDR has increased in visibility and importance as organizations realize that no level of investment will provide 100% protection against threats and as the scale and complexity of the security challenge becomes intractable for individual organizations, regardless of size.

With this growing market demand, some vendors have responded by repositioning existing solutions as managed detection and response. Others have created new and niche solutions, also described as MDR. It's important to understand the needs, perceptions, and ideal value of MDR in order to clearly define it.

NEED

Why do people need MDR?

Security is hard and complicated. Few organizations have the experts and infrastructure they need to protect themselves, and that protection is the most customized part of security. Since they don't feel like they can protect themselves, organizations will rely on other sources and providers to know when they are being attacked and how they can respond. This ability to respond is a natural compromise in the presence of what they see as the impossible task of making themselves 100% secure.

EXPECTATION

What do people believe is MDR?

People think of experts watching screens looking for indications that somebody is attacking them. They think about the experts either automatically stopping the attack or calling them and telling them about it so that they can stop it. Depending on their level of pessimism, they may think of the experts working with them to recover from a widespread attack that has disabled them or working with them to investigate and clean-up after the attack.

GOAL

What should people demand from MDR?

People should step back to think about the outcome they want from an MDR provider. Ideally, they want their systems, that they know are vulnerable, to never experience a successful attack that causes meaningful harm. They should maximize the likelihood of that outcome by setting expectations for what management should mean, what detection should mean, and what response should mean.

To have value, MDR must be continuously informed on the evolution of threats, it must maintain a consistently high level of visibility across all assets, and it must accurately identify attacks in progress to minimize the harm that can be caused. This continuous and comprehensive capability is the most important factor driving organizations to MDR partners. To do this, MDR services require 24/7 visibility, with scalable collection, ingestion, and automated analysis of high-volume, and deep expertise in threat intelligence and analysis to validate events and responses.

MDR Defined.

MANAGEMENT IN MDR

The Management leg of managed detection and response is the most important differentiator between external MDR providers. Responsibility for promptly identifying and mitigating attacks in progress is a serious challenge and requires two capabilities: Operational Competency and Security Authority. Before any vendor can present themselves as providers of meaningful MDR, they must demonstrate both in order to support the security or IT department case for adopting MDR.

OPERATIONAL COMPETENCY

There are five operational elements within MDR that describe Management capable of delivering effective detection and response:

- *The MDR provider has visibility across the environment.*
  Organizations require an understanding of the systems and images that support their objectives to be sure that they see all incidents and understand the scope of any event once discovered. This includes identification of new systems, of critical software revision levels, and insight into traffic passing within the organization.

- *The MDR provider measures the current risk profile and recommends changes.*
  To minimize the potential for successful attacks while simplifying detection of a real incident when it occurs, organizations must have a clear view of their current threat surface in order to remove known attack vectors and needlessly open networks that complicate detection with unnecessary traffic. This profile must identify:
  - » All assets and network locations
  - » Unpatched and vulnerable versions of critical software
  - » Network exposures and impact assessments

- *The MDR provider gathers information from all assets under management.*
  Modern attackers employ attack and infection techniques that spread across multiple system types. Detecting these attacks and understanding their spread requires continuous information from the different types of systems that may be targeted. Reporting on compliance, governance, and risk, also requires information from different systems across the organization. Blind spots allow drift to introduce new areas of exposure on a previously secure system and create havens for long-lived attacks.

- *The MDR provider adjusts information gathering during periods of change.*
  Like attacks, environments are rapidly changing because of technical and corporate evolution, personnel and system alterations, and simple growth. In order to maintain a consistent level of awareness and protection, organizations must be able to reprioritize, reassess, and reconfigure their detection and response tolerances and activities.

- *The MDR provider maintains visibility and interactivity 24/7.*
  Attacks are not limited to standard business hours in any geography and more sophisticated attacks are not strictly serial. A given campaign or exploit can be triggered at any time and individual elements of a complicated campaign may be executed with significant intermediating delays to avoid detection. In order to effectively manage detection and response to attacks, information gathering systems and staff must be continuously monitored to ensure their uptime and responsiveness.

SECURITY AUTHORITY

Security must be understood and managed across multiple technical disciplines to address the wide variety of potential security requirements and security events. For the management of detection and response to be effective in customer environments, the provider must be familiar with the platforms, environments, and threats that comprise these security challenges, demonstrated through:

EXPERIENCE – An MDR provider must have an established infrastructure, processes, and staffing that have been proven to scale and respond with security developments and challenges associated with the service descriptions and levels they are offering. As examples, management must apply to more than a single technology, like EDR, and to threats from multiple vectors against the protected assets. Organizations cannot rely on vendor claims and should seek access to customers and analysts who can speak to management capabilities in real deployments.

INTELLIGENCE – An MDR provider must be able to demonstrate past performance in identifying new and complex attacks, and must be able to describe the process through which threat intelligence and threat identification continually evolves.

EXPERTISE – Recommendations around protective measures, as well as remediation, require ongoing exposure and learning about threat impact and attack mitigation. An MDR provider must have trained and certified personnel who can respond to questions, events, configuration changes, and new technologies.

DETECTION IN MDR

Detection is the element of MDR that requires the most attention, speed, and knowledge. Speed and scope of understanding are important because organizations want their systems, that they know are vulnerable, to never experience a successful attack that causes meaningful harm. There are four elements to the term Detection that define appropriate capability to ensure protection of customers:

- *Detection begins with a comprehensive knowledge of threats.*
  Whether it is understanding exploitable vulnerabilities or recognizing attacks in progress, detection is driven by continuous research performed by experienced analysts who know where to look. This research also enables prioritization of risk from those threats, measured by the likelihood and current instances of these attacks in progress.

- *Some detection occurs prior to attacks and incidents taking place.*
  Minimizing risk includes identifying threats before attacks and incidents occur, by also minimizing exposed vulnerabilities. Detection of vulnerable systems, of insecure configuration changes, and of new unprotected systems joining the network are required to identify and limit those vulnerabilities. To be effective, this information must also be enriched with exposure, likelihood, and severity data, providing a basis for triaging and remediating known issues.

- *Detection is enhanced with human expertise to increase accuracy.*
  Alarm fatigue and false positives lead to analyst burnout and missed incidents. To be trusted and effective, detection must be combined with credible validation prior to any calls for response. The complexity and changing context of some potential security events calls for the intermediation of expert reviewers who can validate events and their seriousness, while enriching them with additional data.

- *Detection must occur in near real time.*
  Reducing impacts and lateral spread requires attack identification in minutes, not hours or days. Automated continuous information gathering and analytics provide high-quality indications of attack for further analysis, eliminating dwell time and improving upon traditional retrospective log and traffic review.

RESPONSE IN MDR

Response varies according to the nature of the security event detected, the value and type of asset under threat, and the outcome desired by the managed organization. In some cases, victims simply want the attack to stop so that they can move on. At the other end of the spectrum are organizations that are more interested in understanding the source and motivation behind the attack; those who are willing to allow an attack to continue in order to examine it.

As a result, response is not a simple activity, but is often a blend of multiple actions, ordered based on the priority of the information or action that each delivers. There are five general response types with associated outcomes and activities:

- **Investigate** – Immediate action is to enrich security event notification with additional data prior to taking any active step to mitigate the threat.

  Example: A new vulnerability is identified within a retailer's ERP system leading up to the holiday season. Patching or isolating the system immediately isn't possible because taking down a revenue generating system at the height of the busy season is a non-starter. The right response is to investigate the exposure of the application to identify appropriate mitigating controls and monitoring changes until a reasonable service window is available.

- **Eliminate** – Immediate action is to disrupt the attack, patch or block access to the vulnerable service, or disable the threatening/anomalous user account.

  Example: A destructive attack, like ransomware, infects a patient admitting system at a healthcare clinic. These attacks can spread rapidly. The right response is to eliminate the attack, by either shutting down the system, killing the malicious process, or isolating all affected devices.

- **Notify** – Immediate action is to inform appropriate responders of the security event with sufficient detail to enable response planning and decision-making.

  Example: A financial services firm's IT administrator's credentials are being used to access and modify systems which were previously untouched. The right response is to notify the admin of the anomaly to ensure this is an approved activity. This could be an early warning to a potential insider threat or could be nothing at all.

- **Contain** – Immediate action is to limit the access of the vulnerable or compromised entity, which may mean limiting system services, restricting network access and egress, or reducing user roles and privileges.

  Example: Privileged credentials of a senior executive are being used to manipulate company information from an unusual geography. The right response is to contain the potential threat by limiting the privileges of the credentials until the executive can be contacted to verify the legitimacy of the activity.

- **Remediate** – Action (usually not immediate) is to address the underlying condition that created the window for the threat, which could be to update policy, change control, misconfigured software, or stolen credentials.

  Example: A new vulnerability is discovered in a widely deployed application on a manufacturer's factory floor, meaning it is installed on multiple devices. The right response is to remediate the vulnerability by rolling out the patches to the affected systems in groups, while applying additional protections and monitoring for the systems waiting to get patched.

MDR MANIFESTO AND YOU

As the threat landscape and complexity of attacks continue to evolve, so will the definition of MDR. We invite you and all security experts, advocates, and champions that embrace the MDR manifesto to share it forward with others in your community. Contribute to the conversation for advancing MDR: ***#MDRmanifesto***