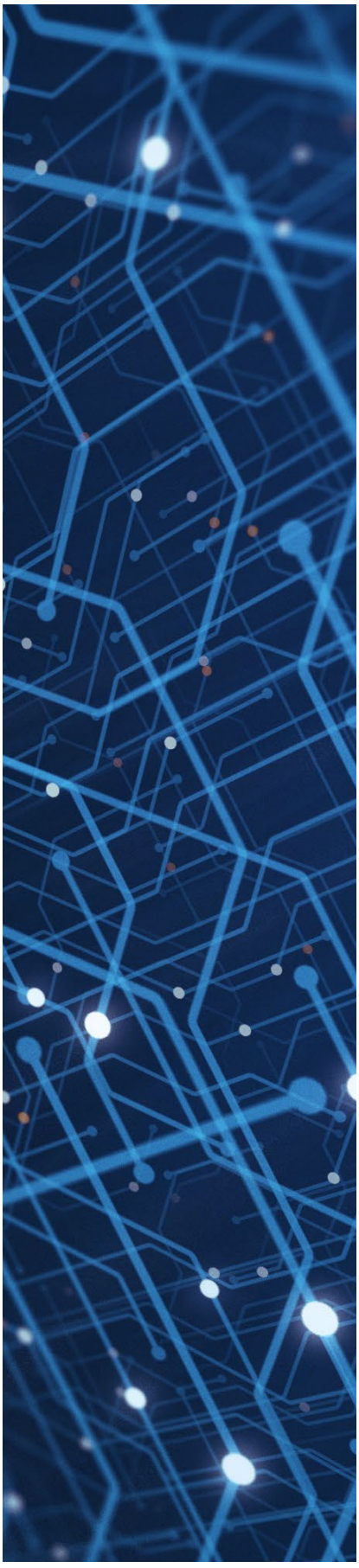
TAG CYBER

opentext™

Managed Detection and Response (MDR): Investigative Capability as a Key Selection Factor

Dr. Edward G. Amoroso
Chief Executive Officer, TAG Cyber
Distinguished Research Professor, NYU

Managed detection and response (MDR) solutions benefit from investigative capabilities, particularly as derived and evolved from the digital forensic community. Buyers should thus include investigative experience as a selection factor when reviewing MDR offerings.



Introduction

The emergence of managed security service (MSS) offerings in the late 1990's was driven primarily by the need for enterprise teams to have experts remotely manage their firewall and review the log records being generated. As offerings from managed security service providers (MSSPs) evolved, and as perimeter-based firewalls became less important, the emphasis of most MSS solutions shifted from device management toward the analysis of collected logs.

In this report, we outline how this shift has resulted in increased emphasis by practitioners on new managed detection and response (MDR) commercial offerings. As will be outlined below, such MDR solutions combine data collection, correlative processing, incident response, and data analysis support for the enterprise buyer. They also help to address the security skills gap by augmenting the enterprise team with outsourced experts.

We also focus in this report on a key selection factor that buyers are advised to consider in their selection of an MDR partner. This key factor, investigative capability, involves the MDR vendor's ability to perform analytic tasks to make sense of the data from managed infrastructure. The case is made here that investigative capabilities, including how such expertise has evolved within the vendor team, is a primary predictor of MDR success.

Baseline MDR Capabilities

The best way to differentiate traditional MSS from evolved MDR is to visualize where these respective offerings reside in the defensive lifecycle model included in the NIST Cyber Security Framework (CSF) . Most observers view any shift along this model as being either a shift-left toward more preventive focus, or a shift-right toward more detection and response focus. Figure 1 below depicts this shift landscape.

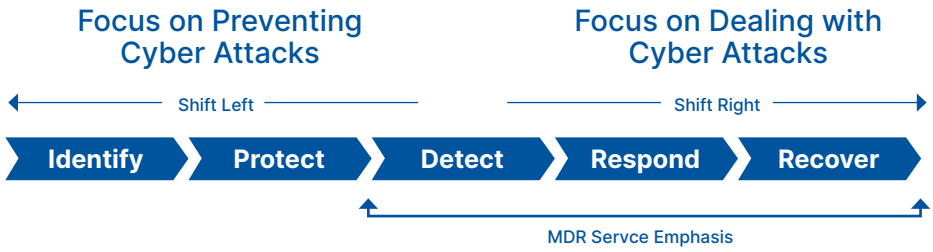


Figure 1. Landscape Shift Options: Left and Right

One of the main reasons MDR solutions have been so successful is that advanced cyber threats have been so difficult to prevent, especially when they are initiated by capable actors such as nation-state military groups. Security teams have had to place their primary focus on addressing on-going incidents, responding to live attacks, or responding to completed incidents with the necessary remediation and recovery actions.

The result has been a definitive shift right in the cyber security industry, with major emphasis on detection and response. In addition to MDR, buyers now have access to solutions for network detection and response (NDR), endpoint detection and response (EDR), and even extended (wildcard) detection and response (XDR). Each of these offerings focuses its attention on dealing with on-going or previous incidents.

[1]https://www.nist.gov/cyberframework

Copyright © 2021 Open Text. All Rights Reserved. Trademarks owned by Open Text.

Investigation as a Key MDR Component

As might be evident in this shift, MDR solutions are heavily oriented toward investigation of incidents versus the earlier focus in previous generations of managed security on prevention and mitigation. This emphasis suggests that the selection process for an MDR vendor should include sufficient review of the local capability for supporting investigation work, based on collected data before, during, and after an incident.

One area where such investigative capability has been particularly highlighted is digital forensics. For many years, enterprise teams, law enforcement, and other stakeholders have used digital forensic methods to investigate the characteristics and data on targeted devices, systems, and software (including stored and ephemeral data). The resulting best practices offer excellent insight into the types of methods that should be included in any MDR offer.

Elements of Digital Forensic Investigation

When law enforcement and other forensic examiners are working a digital investigation, they must engage either explicitly or implicitly with a four-step lifecycle model that includes many discrete tasks. Each task in this model – which is represented below as a de facto guide, rather than a formal standard – is designed to help uncover insights from artifacts, and most are now heavily reliant on technology support for proper execution.

Figure 2. Elements of Cyber Investigation

Step 1: Preservation

This involves freezing any activity that might damage or change important digital evidence. This type of activity applies to MDR offerings, where collected logs, telemetry and other ephemeral data must be stored securely — without the possibility of tampering or damage.

Step 2: Collection

This involves obtaining the digital evidence that will be required for the investigation. MDR solutions have analogous collection capability with the capture of remote logs, audit records, alerts, alarms, and other telemetry from the managed infrastructure.

Step 3: Examination

This involves technical and systematic review and search of evidence relevant to the investigation. Every MDR must include similar examination capability, usually performed using a combination of automated and manual procedures in the MDR SOC.

Step 4: Analysis

This important task involves the correlative and logical review of digital evidence to draw conclusions. Increasingly, MDR solutions use intelligent algorithms to perform the analysis task. Such solutions typically combine the best elements of signature, behavioral, and artificial intelligence-based processing.

Step 5: Reporting

This final step involves documenting findings in a manner useful to all participants in the investigation. Every MDR now includes the requirement to support reporting requirements, often with the nuance that summary analyses be consumable by both cyber experts and business executives.

This analysis of digital forensics methods suggests that any selected MDR platform and supporting vendor should be rooted deeply in proper digital investigative capability. As outlined above, MDR solutions focus on detection and response – both of which are essential aspects of the five-step process for digital forensic investigation. It therefore stands to reason that an MDR vendor must have deep understanding in this area.

Several academic works (including https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.258.7882&rep=rep1&type=pdf) use this basic model to describe digital forensic examination.

Copyright © 2021 Open Text. All Rights Reserved. Trademarks owned by Open Text.

Questions to Ask Your MDR Vendor

The TAG Cyber analyst team recommends that buyers considering MDR options should adjust their conventional source selection process to include increased emphasis on investigative expertise and experience amongst the MDR principals. To that end, we have created a series of simple questions that might be asked of the MDR solution provider to help gauge this level of investigative capability which we believe helps to predict the success of an MDR engagement:

To what degree does the MDR vendor possess direct forensic investigative experience with modern digital scenarios?

Obviously, digital forensics and MDR are different activities, and we fully understand that contracts for MDR will likely not include work items for forensic analysis of devices and other systems. Having local experience with digital forensics, however, strikes the TAG Cyber analyst team as being a good predictor of how well the organization can handle digital review, data analysis, and investigative support.

What platforms and tools is the MDR solution provider familiar with in the context of modern digital forensic investigation?

The desired level of experience with digital forensics across the MDR team should be complemented with an understanding and familiarity with best-in-class tools for supporting investigations. MDR teams might not use these tools directly in their detection and response engagements, but we believe that prior or on-going experience supporting investigation using the best commercial tools is a reasonable requirement for a good MDR team.

What is the MDR vendor's methodology for weaving digital forensic capabilities into their day-to-day detection and response support?

This question does focus on the synergy between digital forensics and MDR support. In particular, it asks the MDR vendor how investigative experience and expertise can be woven into the detection and response activities in support of the enterprise customer. This synergy can be strategic, offering framework guidance on how to design a data analysis program, or it can be tactical, offering more specific step-by-step assistance in dealing with a given task.

About TAG Cyber

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

Copyright © 2021 TAG Cyber LLC. This report may not be reproduced, distributed, or shared without TAG Cyber's written permission. The material in this report is comprised of the opinions of the TAG Cyber analysts and is not to be interpreted as consisting of factual assertions. All warranties regarding the correctness, usefulness, accuracy, or completeness of this report are disclaimed herein.

Copyright © 2021 Open Text. All Rights Reserved. Trademarks owned by Open Text.