SANS

Analyst Program

Spotlight

Unveiling the Invisible: Effective Detection of Advanced Threats

Written by **Dave Shackleford**

October 2023

SPONSORED BY

TATA

TATA COMMUNICATIONS

Introduction: The Need for MDR

For security operations teams, it's been clear for some time that additional operational capacity and expertise to detect and respond to today's threats are needed. In the 2023 SANS SOC Survey, high staffing requirements and a lack of skilled staff were found to be some of the top barriers to fully utilizing a security operations center (SOC) function.[1]

Managed detection and response (MDR) offers an outsourced model of workload and network protection that can help intrusion analysis and investigation teams more rapidly and efficiently prevent, detect, and analyze malicious behavior in their environments by offloading most of the routine security operations tasks to a dedicated service provider. Many enterprises are lacking experts in security operations and don't have enough time to train Tier 1 analysts on the job, so one of MDR's primary goals is to help overcome today's security skills gap through a managed services model. The SANS 2023 SOC survey also found that many SOC teams are outsourcing offensive controls validation (pen testing and red teaming, often for forensics), threat intelligence, and some threat hunting. In line with the staffing and skills challenges that organizations face, highly skilled MDR providers can offer these services readily, helping to quickly mature the SOC in organizations of all types.

Many attacks don't leverage malware at all: Attackers are using memory-resident techniques, compromised credentials, and built-in system tools such as PowerShell to avoid detection by many of the traditional endpoint security platforms.

Effective Detection for Advanced Threats

The threats to our networks, applications, and data today differ significantly from those seen in the past. Attackers are getting smarter and stealthier than ever, and the sheer size and complexity of today's computing environments complicates our discovery and response efforts. Ransomware has become as much of a threat as phishing, based on multiple SANS surveys and reports.[2] Notably, these—the most impactful threats the SANS community is experiencing—occur on the endpoint. Many endpoint security tools and practices in use today are inadequate. The previous generation of signature-based detection tools is failing us. Many attacks don't leverage malware at all: Attackers are using memory-resident techniques, compromised credentials, and built-in system tools such as PowerShell to avoid detection by many of the traditional endpoint security platforms. However, endpoint detection and response (EDR) and next-generation anti-malware tools are better than ever before, so why are we missing these attacks? We need prevention and detection capabilities that go beyond signature detection and can predict and block an attacker's movements before they become impactful, focusing on behaviors that are seen in the wild associated with more advanced threat actors and their campaigns. To better detect and respond to advanced persistent threats (APTs), MDR providers should offer these core capabilities (also shown in Figure 1 on the next page):

[1] "SANS 2023 SOC Survey," June 2023, www.sans.org/white-papers/2023-sans-soc-survey [Registration required].

[2] "SANS 2022 Ransomware Defense Report," March 2022, www.sans.org/white-papers/sans-2022-ransomware-defense-report [Registration required].

- **Near real-time detection—**A mature MDR solution should be able to continuously tune and update detection analytics and rulesets so that near-real-time detection is possible, and any alerts are prioritized for investigation. MDR offerings should ideally incorporate machine learning to better process new threats and manifest detection capabilities to customers quickly.
- **Proactive threat hunting—**All MDR solutions should offer some fundamental hunting capabilities based on indicators of attack (IoAs), indicators of compromise (IoCs) and more advanced-attack behavioral tactics. For most MDR scenarios, threat hunting capabilities will be directly tied to EDR, NDR (network detection response), and SIEM access by the MDR analyst team, as well as event ingestion and analysis (usually in the MDR cloud). Threat hunting across a variety of locations is a critical facet of MDR today, and organizations interviewing potential MDR providers should determine how the vendor pursues threat hunting (proactively, in response to incidents, or both) as well as how the outcomes of threat hunting are applied to ongoing detection and response efforts. Ideally, diverse types of threat hunting are supported (EDR, XDR [extended detection and response], NDR, etc.).

NEAR REAL-TIME DETECTION
PROACTIVE THREAT HUNTING
MAPPING TO MITRE USE CASES
LOG COLLECTION/ STANDARDIZATION/ NORMALIZATION
AUTOMATION AND ORCHESTRATION FOR RAPID DETECTION AND RESPONSE

Figure 1. Core Capabilities MDR Providers Should Offer

- **Mapping to MITRE use cases—**Top MDR solutions should also help identify and close gaps in security operations by correlating detection events to events reported in threat intelligence feeds or mapped to tactics, techniques, and procedures (TTPs) documented in the MITRE ATT&CK® framework. A key indicator of MDR maturity is the breadth of MITRE use cases supported and capably managed for customers.
- **Log collection/standardization/normalization—**The ability to ingest log and event data into a SIEM platform is a critical capability for any MDR provider, and these logs should be normalized for maximum effectiveness in building out correlation cases and applying detection playbooks. Log data plays a critical role in threat hunting as well, so the larger the breadth of log data that MDR providers can ingest, the larger the potential scope of threat hunting endeavors.
- **Automation and orchestration for rapid detection and response—**Another critical MDR feature is the ability to automate more capabilities in both detection and response. Many organizations are already looking to build and implement automation workflows internally to save operational time and reduce the burden of common and routine tasks. In the most recent SANS incident response (IR) survey, 67% of organizations reported a mean time to respond (MTTR) of less than 24 hours, with that number increasing to 95.8% when measuring an MTTR of less than 30 days. MDR solutions are increasingly able to support this goal by integrating with APIs, SOAR (security orchestration, automation, and response) platforms, and cloud provider services. This can help to reduce the time to detect and respond to events, and even perform automated blocking, quarantining, and forensic acquisition activities.

[3] "SANS 2019 Incident Response (IR) Survey: It's Time for a Change," July 2019, www.sans.org/white-papers/39070

It's important for organizations to track key metrics to measure the effectiveness of their threat detection and response with MDR services. In accordance with the critical SOC functions MDR offers, some of the more important metrics to consider with any MDR solutions include:

- MTTR
- Mean time to detect/triage
- Number of SOAR playbooks
- Number of automated hunting patterns available
- Escalation SLAs
- Number of SIEM use cases

Choosing the Right MDR Provider

Consider several factors when choosing MDR solutions. The following is a good starter list when beginning your evaluation:

- **Catalog of MITRE-aligned use cases—**As mentioned previously, MITRE-aligned use cases for threat detection (as well as hunting, forensics, and other capabilities) are a "must-have" capability for mature MDR providers. The MITRE framework is updated regularly, so MDR providers should have a dedicated internal threat analysis team that provides new and updated use case playbooks and workflows to customers as soon as possible.
- **Automation and orchestration for rapid threat hunting, detection, and response—** In alignment with key capabilities mentioned previously, a mature MDR should have a well-tuned and automated threat hunting capability, as well as strong integration capabilities with EDR, NDR, SIEM, and other common tools such as ticketing solutions needed to manage incident investigations, escalation, and more. The more SOAR playbooks and workflows offered out of the box, the better.
- **Threat intelligence capabilities—**Organizations rely on MDR providers to track attack campaigns and adversary behaviors in the wild, so threat intelligence is a major element of MDR offerings both in application to detection and in reporting for further investigation and analysis. MDR is well-suited to organizations that are operationally shorthanded, and threat intelligence is often a luxury for which these types of teams don't have capacity. Adding threat intelligence into the mix of MDR services makes sense, and today more security and IT teams are beginning to focus on attacker campaigns and known adversary groups that target specific industries. More mature MDR solutions offer a mix of automated and human-operated threat intelligence, which can help to increase accuracy as well as dissemination to customers.

- **Global/regional coverage—**For larger organizations that span different regions or the globe, it's critical that any MDR solution be capable of monitoring all locations at all times. For many organizations, too, it's common for different business units or groups in different regions to leverage a variety of security technology, so MDR solutions should be capable of accommodating existing on-premises SOCs, managing or co-managing SIEM platforms, or enabling hybrid SOC capabilities and features as well.
- **Expertise of analysts—**Ideally, providers will require industry certifications or other accreditation for their analysts such as the CISSP, GIAC certifications, or others. Potential customers should emphasize a background with the tools they actually have in place (such as EDR or a specific SIEM) and inquire about expertise and skills with them.
- **Add-on or premium services provided by vendors—**Some providers offer a range of consulting services in addition to their core MDR capabilities, including forensics investigations, dark web monitoring, malware analysis, full SOC replacement, vulnerability scanning and penetration testing, and others. Similarly, some providers are now starting to offer "hands-on-keyboard" response services that involve human analysts. More advanced services that focus on fraud detection and brand monitoring are becoming highly sought after, as are specialized technical capabilities such as red/blue teaming, advanced threat hunting, and specialization in IT/OT threat hunting and investigations.

The goal of any MDR is to make security operations more streamlined and simpler for an organization that is likely taxed to begin with. As such, ease-of-use and the ability to rapidly drill into data provided by the MDR analysts is paramount. With the ongoing operational constraints many SOC and investigation teams face today, it's likely that the MDR market will grow rapidly in the next several years and become more agile and capable at the same time. The range of tools and services supported by leading MDR solutions is expanding quickly, and the integration of threat intelligence, threat hunting, and automation playbooks will only see MDR becoming more valuable in reducing the time to detect incidents, respond or escalate events as needed, and provide reporting quickly on evidence discovered and overall security trends observed.

Ease-of-use and the ability to rapidly drill into data provided by the MDR analysts is paramount for an MDR.

Sponsor

SANS would like to thank this paper's sponsor:

TATA

TATA COMMUNICATIONS

About Tata Communications

A part of the Tata Group, Tata Communications (NSE: TATACOMM; BSE: 500483) is a global digital ecosystem enabler powering today's fast-growing digital economy in more than 190 countries and territories. Leading with trust, it enables digital transformation of enterprises globally with collaboration and connected solutions, core and next gen connectivity, cloud hosting and security solutions and media services. 300 of the Fortune 500 companies are its customers and the company connects businesses to 80% of the world's cloud giants. Its Tier-1 IP network, wholly owned subsea fibre backbone and consortium cables' global network carries ~30% of the world's internet routes. With its award-winning capabilities Tata Communications cyber security portfolio spans Advanced Network Security, Cyber Threat detection and Response, Cloud Security and Security Assessment & Consulting that helps organizations become cyber resilient.