DATASHIELD™ | an ADT company

SOLUTIONS GUIDE: Managed Detection & Response

MSSP vs MDR

In the new cyber landscape of "Security as a Service" many Managed Security Service Providers (MSSP) claim that they can deliver Managed Detection and Response (MDR) type services. What is the difference? How can you ensure your organization is truly safe while managing your security tools effectively?

Before we jump into the key differences between MSSP and MDR services, let's first examine how they are the same.

> As Gartner puts it: *"The overlap between managed security services and MDR is increasing, which is adding to the confusion in the market and making it difficult for buyers. MSS and MDR still have distinct characteristics that buyers need to understand."*

Both provide 24x7x365 outsourced monitoring of security devices and systems. This also typically includes some level of event logging, compliance reporting, incident response support and containment.

Great...so how do they differ and which should you choose?

> *As Anton Chuvakin Research VP and Analyst for Gartner summarizes "...an MDR is simply an MSSP that knows how to detect actual threats..."*

What does this mean to your organization? It means with an MDR you will spend less time sifting through alerts and less money on the people, technology and time to do so.

How can an MDR deliver on this promise? A true MDR has the technology, expertise and experience to provide a complete forensic investigation, only notify the customer when true events arise and help initiate an action plan with remediation recommendations if necessary.

Outlined below is an example of the difference between a traditional MSSP and MDR in how they handle actual customer incidents.

EMAIL ALERT
SENT FROM IDS

From: security@example.net
[mailto:security@example.net]
Sent: Wednesday, February 13, 2019 6:55 AM
To: <Client Name>
Subject: Incident #1803420: Trojan infected system at x.x.x.x

Incident ID 1804460 created on Feb 13 2019 6:54am GMT

Client: XXX
Appliance: xxxxxxx-ids-01
Status: Open
Threat: High
Class: trojan-activity
Start Date: Feb 14 2019 6:54am GMT
End Date: Feb 14 2019 6:54am GMT

Summary: Trojan infected system at x.x.x.x

MSSP

Alert Customer - A Trojan had infected a system

[jdoe@example.com]----------
------[Feb 13 2019 6:54am GMT]

The system at x.x.x.x (ex3. local.example.org, MAC: 00:00:00:aa:00:7e) appears to be infected with a trojan. It is making zero byte POST requests to IP xx.xxx.xxx hosted in Hong Kong.

ISSUES WITH MSSP ALERT

- No additional details included
- No indication the MSSP actually investigated the alert further than reading the initial alert
- No remediation assistance
- Alert prone – alerts client of any and all alerts regardless of false-positive findings

DATASHIELD™

- ✓ Forensic Investigation – Detailed investigation resulting in complete story of infection with forensic details.
- ✓ Provide Complete Investigation Story Write-up – We share the story of this infection with the Client.
- ✓ Notify Client (If Warranted) – Only warranted investigations are sent to the Client.
- ✓ Provide Remediation Recommendations – Every investigation includes an action plan of how to remediate the issue.

We recommend x.x.x.x be taken offline and scanned with your antivirus to isolate this infection. Please let the MDR SOC know how we can further assist you with your investigation.

This investigation will remain open for 72 hours unless you decide otherwise.

DATASHIELD™ MANAGED DETECTION & RESPONSE

Lack of budget coupled with a shortage of resources makes it increasingly difficult to implement a security program capable of:

- Comprehensive 24x7x365 continuous monitoring
- Full network visibility beyond signatures and logs
- Real-time advanced threat detection using cyber threat intelligence
- Active Hunting
- Deep Forensic Analysis

DATASHIELD's Managed Detection and Response service operates as an extension of your security team, providing the required expertise and resources to identify even the most advanced threats. The DATASHIELD approach allows the customer to focus on validated threats only, which reduces the complexity and cost of threat detection. Working in partnership with your business, Datashield will validate incidents, provide relevant context, investigate to determine scope and severity, and make recommendations for immediate containment and response.

> *"Customers want an all-inclusive service when compared to many MSSPs, they receive a significant amount of false positive alerts, and the alerts that are valid have minimal information, so they are left to fend for themselves"* **– Jeff Marshall CISO Datashield**