WHITEPAPER

Sophos Managed Threat Response

Manage Threat Response
Sophos MTR Analysis

Introduction

This document outlines my view of customer positions that I observe, and how the features of Sophos MTR can be used to quickly, easily, and comprehensively fill some of the large gaps within IT security that are understandably subject to a paralysis of decision making.

SOPHOS
Cybersecurity delivered.

pavilion

The reality, and challenge!

Many customers I speak with have an IT team that are very thinly stretched. Let's face it, nobody's IT team have available capacity and are always being challenged to do more with less, and have to make priority calls on which topics to address and which will have to wait. Security is a non-negotiable priority, but it can be easily overlooked or put on the back-burner. Sometimes this is not for the want of trying. The number of products in this space continues to grow, and these solutions are typically complex in nature and come with significant price tags associated. So, decision paralysis can set in; wanting to ensure the right product is chosen to meet needs, but with the complexity and specialist nature, needing to find time to do enough due diligence in the investigation, understanding and selection.

This is then coupled with BAU security activities (patching, audits, reviews, reconfiguration) which can take significant time in themselves, and follow unpredictable timescales. Big named vulnerabilities like SolarWinds and Exchange in recent months, to name only two in a very long list, force reactive behaviour to address these issues, detracting from regular BAU and planned project work. These types of challenges show no sign of slowing down.

Additionally, there is undoubtedly a need to keep up to date with developments in the cyber security space as well, as it continues to evolve. Staying on top of the following, and how they may affect your organisation:

- The latest vulnerabilities and threats
- The latest exploitable techniques and trends
- The latest updates that are available and consequences/implications of deploying these
- The latest security best practice

All these areas need to be addressed with minimal impact, staffing effort, time, and cost.

Cloud services can help with some of these, by keeping systems automatically updated and patched, but this very benefit can also hinder in other areas. For example, the rapid rate of change that features are introduced, or upgraded, or even retired, and the need to keep on top of these to understand the security and user implications.

An offering to help

Most IT teams need help with these areas and more, and when we are looking at solutions that help our clients (and us!), we look for solutions that are elegant and have smooth integration and excellent functionality and efficacy. It is not always easy!

There are many security products on the market that either rely on pulling logs and data from a wide range of network devices, or that sit in the communication path of devices and capture and analyse traffic as flows. These tools are very clever, and do have a place, but tend to be costly and complex to implement, support and manage/run.

The Sophos Managed Threat Response (MTR) service is a solution that fits what we look for, perfectly. We see it delivering huge value with minimal implementation effort and is a service that can give you additional peace of mind over your organisation's IT security.

The Sophos MTR service extends the Sophos Endpoint solution, so for existing customers the implementation is incredibly easy. For customers that are not protected by Sophos then a simple agent can be deployed to the endpoints to enable the functionality. This will allow you to continue using your existing security solution in addition to being protected by Sophos MTR. All the agent and configuration management is done via the Sophos Central Cloud portal, which will be familiar to existing customers, and incredibly easy to learn for new customers!

Sophos MTR is a managed security service that utilises passive and active threat hunting, using data science/big data analytics to stay on top of clearly identifiable threats, coupled with expert human engineering to detect threats that are more subtle and nuanced. All this is run by a 24x7 operational team. In addition, the MTR team will also ensure that your Sophos endpoint settings are optimally configured, to ensure you are not missing out on any best practice settings, or new features that are paid-for but not yet applied.

There are several models of engagement with the MTR team, depending on your teams' skills and capability:

- The MTR team can **notify** you when a threat is detected, allowing your teams to react and deal with this in the most appropriate manner.
- They can **collaborate** with your teams, working together to remediate the issues.
- Or they can be **authorised** to take immediate action, to isolate and respond to the issue and then will keep you fully up to date with the actions taken.

The Sophos endpoint solution stack

For customers that are already protected with Sophos, MTR builds upon the current solution sets.

- Sophos endpoint - This is the standard endpoint protection, and in my view should always be considered with Intercept X, the anti-malware component
- Sophos endpoint with EDR - Endpoint Detection and Response - This extends the endpoint agent features and provides tooling for rolling your own Endpoint detection and response service. It allows for threat hunting, detecting indicators of compromise, auditing, and reporting on your endpoint estate. This is a very comprehensive toolset that gives administrators and IT security engineers significant power and information available at the click of a button/run a query.
- Sophos MTR - this builds upon the EDR toolset, and essentially provides a managed EDR service. For customers that want the functionality of the EDR toolset, but do not have the skill or time to up-skill and maintain the specialist knowledge in house, this option provides a specialised Managed threat response team of experts that can run that for you.

The security onion

In my view the benefit of utilising the agents on the endpoint is that this is mostly likely where threats will be targeted. Whilst it is undoubtedly very helpful to gather data from as many sources as possible, the interaction and execution of malicious activities will normally be on the endpoints (computers or servers). This is where users will download malicious files to, it is where malicious links will be clicked, it is where threat actors would want to deploy malware to capture keystrokes, or data or cause their disruption, it is the richest resource of vulnerabilities! By ensuring your endpoint activities are being analysed, you are protecting against many likely attacks. Security is very much like an onion, with many layers all playing their part. If something did make it through all the preceding layers, to the endpoint, then Sophos endpoint can detect it, and with Sophos MTR providing proactive and reactive analysis, 24x7, you bolster and increase protection so that your organisation can thwart attacks, and you can sleep more easily at night!

Pete Clements.

To learn more about how PAVilion can help support your organisation, please contact info@pav.co.uk

Pavilion
The Old Corn Mill, Bullhouse Mill
Lee Lane, Millhouse Green
Sheffield S36 9NN

Tel: 01273 834 000
Email: info@pav.co.uk
URL: www.pav.co.uk

SOPHOS
Cybersecurity delivered.

pavilion