academia
the technology group

smartdesc
part of
academia the technology group

Managed Detection, Response and SOC

CYBER ESSENTIALS
Microsoft Solutions Partner
Security
CISSP Certified Information Systems Security Professional
National Cyber Security Centre
SOPHOS

Academia's Managed Detection and Response (MDR) + SOC Service combines round-the-clock proactive threat monitoring, response & intervention with vulnerability management and human led specialist cyber advice and guidance as a complete service; drastically improving your cyber security posture and resilience. The service leverages the power of Sophos – a UK company and the leading global provider of cybersecurity services and interweaves our own expertise and support. This unique combination delivers a holistic service that not only guarantees you best-in-class protection 24x7x365, but also ensures you have the specialist resources available to deploy, manage, advise and maximise value in the platform.

What is included?

24/7/365 Threat Monitoring

A team of experts watching your environment to identify suspicious behaviours that may indicate a compromise or breach.

Cyber Incident Response

Immediate threat containment and full-scale incident response to neutralise threats and establish root cause - with no caps on hours spent, or additional fees.

Threat Intelligence

This involves using threat-focused analytics to identify emerging threats. Continuously update and apply detection rules based on current threat intelligence to stay ahead of evolving threats.

Elevated Threat Detection

Detect and stop more cyber threats than security tools can identify on their own.

Vulnerability Overwatch

Provide visibility across endpoint, firewall, identity, email, network, cloud, backup and other IT tools.

Expert-led Threat Hunting

Focused on finding "unknown unknowns" (i.e., threats not currently detectable by current prevention or detection technologies).

Human-led Cyber Advice and Guidance

Regular one to one review meetings with our dedicated, in-house cyber specialists, to help you understand the key risk areas in your estate, make sense of the telemetry dataand continuously evolve your cyber security strategy.

Academia's Managed Detection and Response (MDR) Service is a simple, yet effective solution, that monitors your estate around the clock and with trained security analysts and threat hunters responding to any threats against it.

Our MDR Service covers not only your endpoints and servers, but also your network and a wide range of cloud platforms and services:

Windows Clients | Mac OS Clients | Linux Clients | Microsoft 365 | Windows Servers | Google Workspace | Jamf Protect | Okta | Cisco Meraki

and many more!

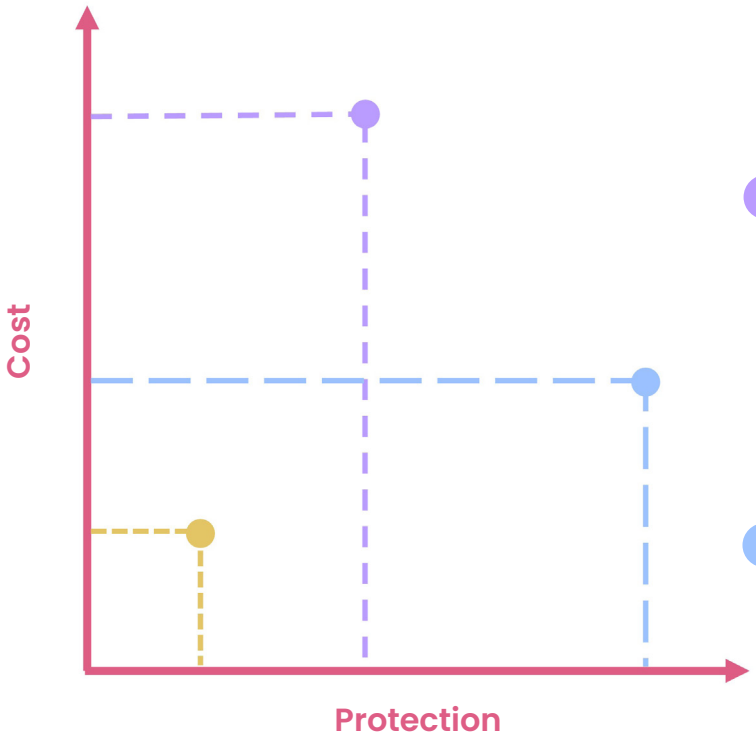
This sounds expensive?

Protecting and maintaining your organisation's operation or mission statement from a security perspective is multi-faceted and sometimes the cost of this may seem like a rather large expenditure when presented in black-and-white figures. However, analysing and assessing your security posture is based on risk versus reward and your security budget and spend needs to be weighed up against the risks of lost business, decreased funding from donors, the ability to fulfil your services to those who need them, or any reputational damage that you may suffer because of an attack or breach.

When considering the requirements for protecting your environment, there are two things you need to take into account; **suitably qualified staff** and a **multitude of systems** to help the staff detect and respond to threats - both come at an individual cost and have varying degrees of complexity and considerations to factor in.

Academia's MDR service covers both for you; and at significantly less complexity to you and those involved in the upkeep of your IT estate and more often than not, at a lower cost than doing it in-house.

The Balancing Act of Your Security Investment:
General Overview



In-house tools + In-house staff (8/5)

Using your existing security tooling monitored by your in-house IT Teams juggling multiple tasks and priorities can lead to security blind-spots, especially outside of the working day (when cyber criminals like to attack!).

In-house tools + In-house staff (24/7)

Bolstering the monitoring of your existing security tooling by standing up an "internal SOC" or having on-call tech staff can help increase your protection levels, but also increase your costs. In some cases, these staff may not be trained security analysts or seasoned "threat hunters".

Academia MDR

Academia's MDR service increases your protection levels by having trained security analysts and threat hunters watching over your environment 24/7/365 keeping the bad guys at bay, whilst potentially reducing your overall spend (and not having to worry about things like annual leave or national insurance bills!).

The bottom line

Endpoint Protection by itself is the cheapest option, but only protects your clients and servers. You will need a team to monitor the output of these tools and know how to handle advanced threats or full-blown attack to truly benefit from them.

Threat Actors like to attack organisations outside of UK working hours or during public holidays when IT Teams are less prepared or not around. Standing up your own "out of hours" SOC costs significantly more money, planning and scheduling.

Academia's MDR service is "more expensive" when compared to standard Endpoint Protection alone, but typically works out to be more cost effective from a TCO perspective, whilst greatly enhancing your ability to respond to threats with a human-led service that is formed of true security analysts who are equipped for every eventuality to protect your organisation against the latest cyber threats.

How the service is delivered

Every organisation is different and we understand that. This is why we offer various "flavours" of our MDR offering to fit any organisation's requirements. How we determine which flavour works best for you starts with a conversation and how much (or how little) you want to be involved in the response actions when a threat is detected.

Essentials

As a Sophos Platinum Partner, we can provide the software to your team at up to 30% below market rates. This gives you full access to the Sophos MDR Complete platform, including the 24x7x365 SOC and Incident Response, for you to implement across your organisation.

Supported

Our Standard package includes the Sophos MDR Complete platform – supplied, deployed and configured by us. It also includes monthly reporting & insights and dedicated time from our in-house Cyber Security Specialists every quarter, helping you understand the priorities being identified by the platform and how to act on them. Plus, access to those same experts ad-hoc when you need it in an urgent situation.

Premium

Our Premium package includes everything in Supported and adds continuous Vulnerability Assessments of your estate in real time. It also includes regular gap analysis of your Microsoft 365 Secure Score and Defender security configuration against Best Practice - helping you stay secure in a constantly changing technical landscape. The Premium plan increases your dedicated access to our Cyber Security Specialists to monthly workshops and comes with regular insights into the wider Threat Landscape – helping to inform and update your Cyber Strategy on a continual basis.

How we handle incidents for critical systems and resources:

Our rule of thumb:

If there is an active incident or attack – we stop it in its tracks.

Why is this our approach?

Not handling an attack in a correct and timely manner may result in the attack spreading further across your organisation, resulting in further infections, or unwanted data access or leaks. Isolating and remediating a threat should always come above considering the implications of the targeted system's availability.

But what if the system is mission critical?

Stopping an attack takes priority and in some cases, this may result in the system(s) being offline for a period of time whilst we remediate and remove the threat. As part of your onboarding onto our MDR service, we work with you to create "Runbooks" which detail each critical system's purpose, the business impact of it being unavailable, the process to take to return it into action and any associated communication plans. These Runbooks are crucial to our service as they help us return you to business-as-usual!

What you get:

More than just Endpoint Protection

Endpoint Protection (or "anti-virus" software) has been protecting us for decades. But as threats evolve, so does the complexity of understanding and actioning what these tools are telling us. What's more, is that the "bad guys" aren't simply targeting only our devices (endpoints) anymore, instead, turning their focus to your user's cloud accounts (i.e., Microsoft 365) that host all an individuals' email, Teams messages, internal intranet sites (SharePoint) and user and shared company files. Our MDR offering covers you on both of these areas and more!

Around the clock monitoring and remediation

With more devices, user accounts and data stored on our networks or cloud locations, having eyes everywhere is not a simple task, let alone being able to identify the suspicious from the normal! It becomes even trickier when all trends point to cyber criminals attacking organisations outside of their working hours, on weekends, or public bank holidays. Our service gives you the visibility, coverage, intelligence and the people to protect your organisation.

Breach Warranty Protection

In a scenario where the tools cannot prevent a ransomware attack in a healthy environment, you can receive up to $1 million "Breach Warranty Protection" from Sophos, showing their commitment to the effectiveness of the solution. This is another step towards securing your organisation financially against the impact of cybercrime - as an addition to your existing Cyber Insurance policy (who look very favourably on MDR!).

A trusted Security Advisor

Academia Technology Group have a combined experience of 40 years servicing our customers across all sectors, from education, to enterprise, large charities, to newly formed Non-Profits. Throughout this, we have not only built our own in-house security teams to support our customers with their Information Security and Data Governance strategies, we are also an accredited IASME Cyber Essentials awarding body. We have also built an extremely strong repertoire of trusted security partners who can help you fill any gaps that you have identified, or we have supported you to identify.

Everyone likes statistics!

Academia will happily walk you through the benefits of adopting a Managed Detection and Response solution as we are technicians who love seeing our customers succeed through the use of well adopted and secure tech. However, to help illustrate the benefits of our MDR solution, here are a few stats surrounding one of the most common and dangerous attacks present today, **ransomware**, that will put the importance of a fully-fledged solution such as MDR into perspective.

Root causes of an attack

29%
of attacks were caused by **exploited software vulnerabilities**

21%
of attacks were caused by **Phishing** attacks leading to compromised **credentials**

40%
of attacks came in via a **previously unknown gaps in security!**

The cost to an organisation

30%
of organisations who suffered a ransomware attack, **also had their data stolen** by the attacker

48%
of organisations ended up **paying the attacker the ransom demands**

£742,000
is the average an organisation **paid to recover their data**

The timings of an attack

31%
of Ransomware attacks occur **outside of normal business hours**

26%
of organisations said it took **up to a month to recover** from a ransomware attack

62%
found that a **lack of people and/or skills hindered their ability** to detect and stop an attack in time

Human impact of an attack

40%
of IT Teams reported **increased pressure from SLT** about their security posture

31%
of IT Teams experienced **staff absences due to stress or mental health issues** relating to an attack

27%
of organisations who were hit by an attack **replaced their team's leadership** post-attack

Get in touch!

Academia Ltd
01992 703 900
info@academia.co.uk

The Progression Centre, Mark Road,
Hemel Hempstead, HP2 7DW

www.academia.co.uk