daisy.

YOUR 10 MINUTE GUIDE TO MANAGED DETECTION AND RESPONSE

Cyber Security

INTRODUCTION

It is estimated that global cyber security spend will continue to rise in 2023, growing by 11.3%. To those in the know, this comes as no surprise, given the increasing volume of attacks organisations continue to face.

Contributing to this are the ever evolving ransomware threats, which have advanced in recent years to not only encrypt data and cripple IT systems but also to steal and withhold critical data until a ransom has been paid.

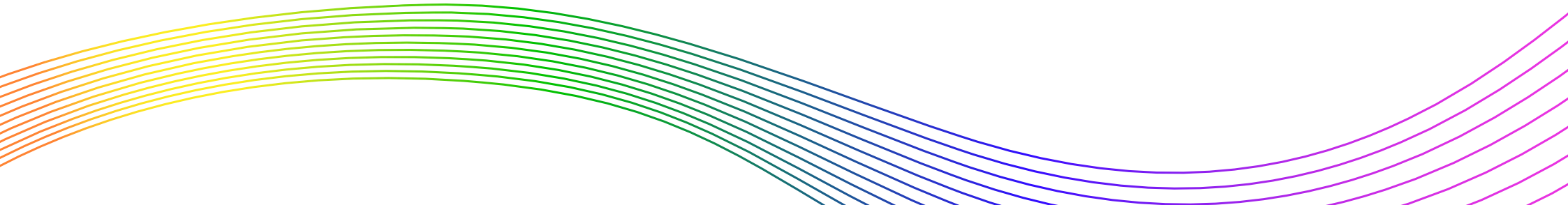
Combined with phishing attacks, which show no signs of going away any time soon, there is now more than ever, a need for organisations to have robust cyber security defences.

With most cyber incidents, criminals are looking for the easiest way to obtain access and will take advantage of any opportunity that presents itself. From our 20+ years experience, we can safely say hackers are not targetting those organisations they perceive to be the most lucrative or where they can be the most disruptive; but are looking for any way in and seeing where it takes them – this means that organisations of all sizes, whether known or not, are at risk.

One of the most effective ways to protect your data and that of stakeholders is to have true 24/7/365 cyber detection in place to alert you to potential threats; allowing your team or the external experts to intervene at an early stage and prevent any potentially costly or even irreparable damage.

Sadly without such solutions in place, many breaches remain undetected until ransomware, or similar, is deployed leaving you locked out of your essential systems, and paying a hefty

One of the most effective ways to protect your data and that of stakeholders is to have true 24/7/365 cyber detection in place to alert you to potential threats; allowing your team or the external experts to intervene at an early stage and prevent any potentially costly or even irreparable damage.



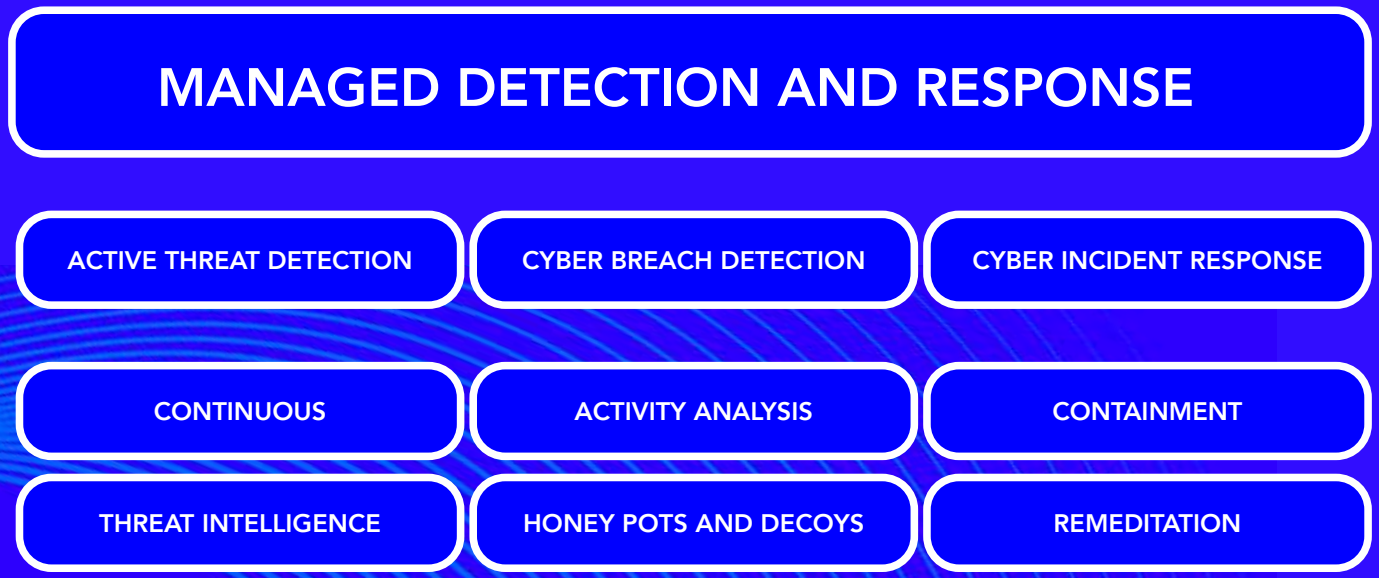
DAISY'S DEFENCE SOLUTION

Our MDR service is supported by our Security Operation Centres (SOCs) located in the UK and Australia. Our locations are selected based on their trusted government and regulatory environment, and availability of highly skilled and qualified personnel.

Our SOCs are designed to provide you with a comprehensive cyber security function, delivering a level of expertise, experience, and technologies that you would find near impossible to replicate in-house. This gives you continuity of service, without the challenges of recruitment, retention, and continual replacement of sought-after cyber security skills.

Drawing on over twenty years' experience, our Managed Detection & Response (MDR) approach is designed to be at the forefront of security services and ready to handle any cyber threats.

SIEM? SOAR? EDR? NDR? XDR? IDS? MDR? Unsure of what the difference is between all of the detection options out there? The reality is, the terminology tends to be marketing jargon and the services provided tend to be quite similar. As with all our communications we opt to keep things uncomplicted and quite simply refer to our service offering as MDR.



MDR SERVICES – IN A NUTSHELL

ACTIVE THREAT DETECTION (ATD)

Combining two essential elements to monitor, analyse and alert you to weaknesses that hackers can see in your internet-facing IT systems.

Unlike traditional penetration testing services, ATD gives you a 24/7 service that alerts you before the hackers have a chance to exploit your weaknesses.

Incorporating Continuous Testing, which scans your connections and tests your configurations daily, with Threat Intelligence to identify system changes and vulnerabilities that could lead to a breach, our ATD is the first pillar in improving your cyber security and staying ahead of hackers.

CYBER BREACH DETECTION (CBD)

Monitoring of security alerts, initial analysis, alerting your internal team and giving advice, support and guidance.

This allows you to identify breaches more effectively and enables you to react immediately in the case of an incident.

CYBER INCIDENT RESPONSE (CIR)

Escalation of important events to our Incident Response Team, supporting with incident management, investigations and external communications.

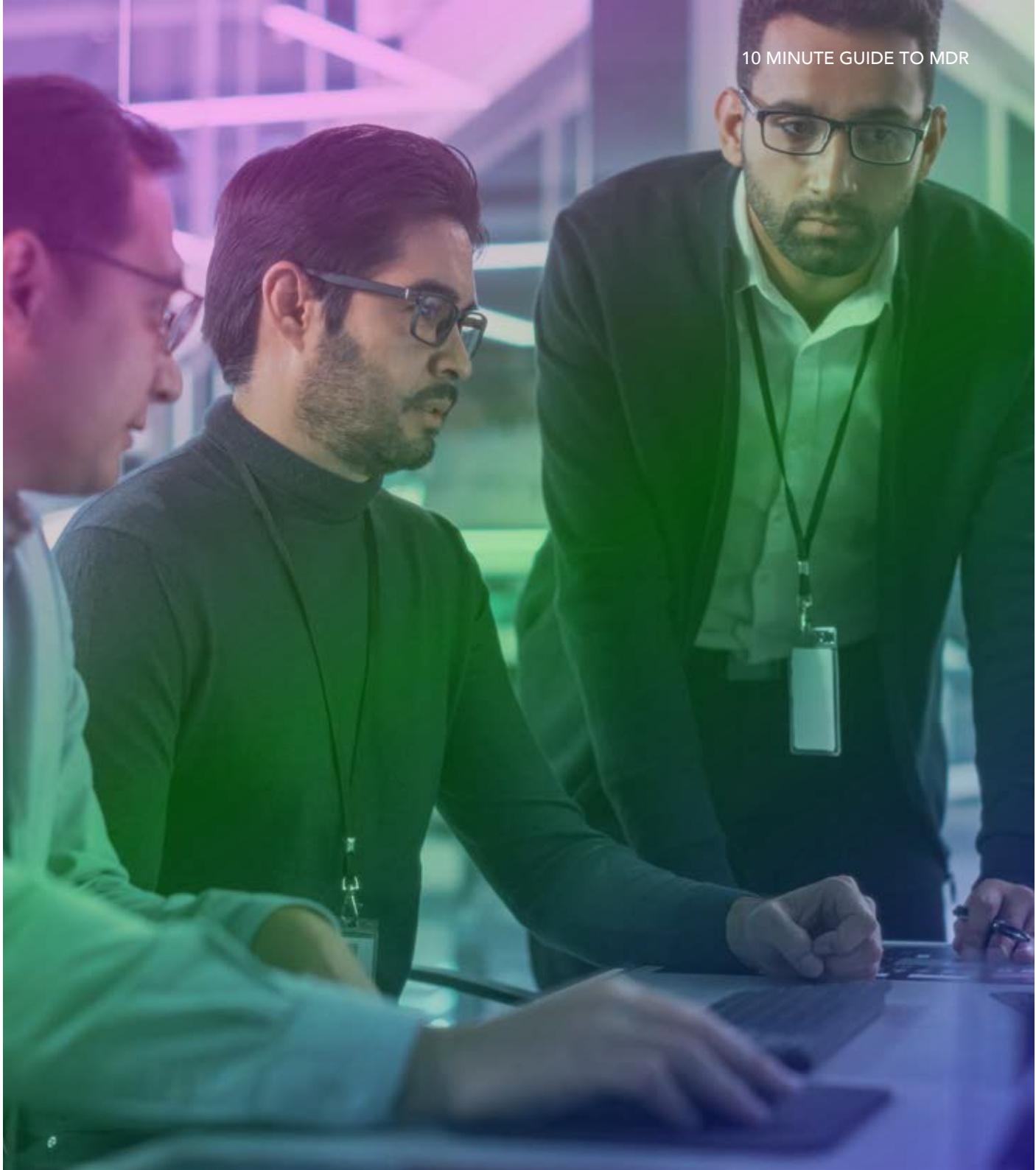
Our team of experts will work alongside you to detect and contain the attack, minimise the damage and prevent future attacks.

WORKING TOGETHER

To ensure our customers receive a 'best-in-class' service, our team of experts consider themselves an extension of your operations team.

Our approach:

- Consultancy led – we work with you to understand your requirements, what you need to achieve and how we can support you on your journey, providing bespoke solutions.
- Dedicated resource – every customer has a dedicated Account Manager and Technical Lead to work in collaboration.
- Partnership – We have a robust and tested onboarding process. Through the extensive tuning phase, your Technical Lead will work with you to ensure the solutions meet your needs.
- Communication – regular meetings, including technical presence, keeps tuning of the service a priority and allows any changes in your environment to be considered for updating threat models.
- Full service provider – We can provide support with managed cyber solutions as well as testing, certifications and meeting security standards such as ISO 27001.



DESIGN PROJECT CASE STUDY

Daisy Design Projects are designed to provide insight for organisations who aren looking to implement and manage a MDR solution in-house, outsource to a third party or simply need help knowing what to include within a tender/RFP.

The aim is to guide organisations to choose the right service for them by inviting them to a 1:1 workshop with our in-house experts.

Here is what one customer thought:

Sector: IT Software
Head of Information Security

› What problem were you trying to address/solve?

Our current solutions required continual management and a dedicated member of staff to monitor and investigate alerts. Long term this wasn't viable given the time this took away from other areas of the security environment that needed attention. We wanted to find a solution that would allow our in-house security team to focus on the day-to-day tasks and allow us to operate a more proactive security environment, rather than a reactive one. We also wanted to offer our business, and customers the peace of mind of having a focused and dedicated 24/7/365 coverage.

› How did you find the session on the day? Anything you would do differently?

The session went well and was informative. If we were to do it again, I would involve more of the team, so they could ask more targeted questions for their specific areas of the business. They would also be able to provide more clarity and content to questions asked by the technical team.

› Do you think the content was at the correct 'technical' level? Explain.

Yes, the content was pitched at the right level. It was easy enough for members of the team who didn't have a technical background to understand but was also expanded to give more depth to those needing the technical content.

› Did you achieve everything you set out to?

Yes, we did. It was also beneficial to attend in person, so we had the opportunity to see the SOC and get to meet members of the team.

› What are your next steps on your cyber journey?

Our next step following the design project was to take the information and details to senior management, to get the project signed off. Once this was achieved, our next steps were to implement the managed service. On completion of this project, the security team can start to look at focusing on other areas, with the peace of mind that should an incident require our attention, this will be flagged immediately for us to deal with.

daisy.

NEXT STEPS

If you want to find out how Daisy can help you to improve your cyber security, contact us on:

0344 863 3000

Or if you're an existing customer, get in touch with your account manager directly.

daisyuk.tech