// Managed Detection and Response

We are your first line of defence against unauthorised actors and threats attempting to cause harm

You've seen why 50% of organisations will have adopted Managed Detect and Response, or MDR, by 2025. Now will you be one of them? Some trends really aren't worth following. But this one is. And when you choose MDR from Cyberfort, you'll make the trend your own.

Our MDR security platform is considered an advanced 24/7 security control that includes a range of security activities including cloud-managed security for organisations that cannot maintain their own Security Operations Centre (SOC). Our MDR services combine the latest data analytic technologies, threat intelligence and cyber security expertise in incident investigations and responses.

Cyberfort's MDR service was designed from the ground up to help IT and security teams with varying degrees of knowledge and skills to strengthen their security posture. Our team of experts will find and stop attackers as well as thwarting them from entering your network and will stay ahead of emerging threats. We use a combination of security expertise and the latest technology solutions to detect dynamic and real-time threats quickly across your entire estate to provide 24/7/365 monitoring, proactive threat hunting exercises, effective incident response support, bespoke security advice and guidance and a team of cyber security experts to stop malicious activity and help you continually improve and harden your security posture.

Above all else, our MDR solution will enable your team to focus on what you're good at, while we give you the peace of mind through our threat detection and response activities. We are not only a supplier to you but we want you to think of us an extension of your IT and security teams. We are your partner in your security success story. Allow our MDR solution to help drive your security program and eliminate fatigue and strain on your analysts to provide more value to your business.

Why you should consider an MDR Solution for your business:

- Many organisations have attempted to establish their own Security Operations Centre and have failed through lack of strategy and the overarching costs associated with building from the ground up.

- Some organisations have bought the latest platform, but they failed to appreciate the level of resource required to operate the platform both from a financial and skills perspective.
    - Leading to alert fatigue
        - Too much data to manage
        - Unable to prioritise alerts
    - Analyst's suffering burnout

- Lack of support from the C-Suite – SOC's are cost centres which spend money but do not generate revenue and therefore most CISO's and Senior Management fail to buy-in as there is no way for them to accurately quantify how much is saved through the prevention of a malware attack or phishing campaign, the only time that an organisation will be able to quantify the financial and reputational impact is post a breach.

- Lack of security capabilities in-house – Lots of organisations struggle to go beyond a prevention focused security strategy and do not have the ability or capability to stand up and maintain their own security operations program.

- Financial investment - The cost of running a 24/7 SOC is over one million pounds per year. Beyond staffing costs, clients need to consider hardware, software and licensing costs and training.

- Team of qualified and experienced experts – Many organisations who take on the task of building their own security team find the biggest challenge in recruiting the best talent and then retaining them. Those organisations who overcome the recruitment and retention challenges, frequently face alert fatigue through poorly developed use cases and rules. Leading a lack of detection and a failure to get a ROI.

- Identifying and categorising risks to correctly target incident responses and drive the systems improvement roadmap

- Log files and events generated by IT systems often provide an extremely useful audit trail which aides in identifying the cause of cyber security breaches and can also be used to detect security incidents or suspicious activity.

- Since the pandemic there has been an increased number of remote employees who are no longer working from a secure controlled environment, with many distractions of from their home life.

Get a fully personalised service that includes monitoring of your notifications and access to operators 24/7/365

What we do

Monitor:

- Endpoints
- Network devices
- Servers
- Mobile devices (data collected from Office 365)
- Internet of Things (if device has ability to push out logs)
- Cloud services (Office 365, Amazon Web Services, Microsoft Azure, Google Cloud)
- Firewalls

Detect:

- Cross-platform malware
- Botnets
- Ransomware
- Behavioural ransomware prevention
- DLP monitoring
- Spear phishing and Whaling
- Watering holes
- File Integrity Monitoring (FIM)
- Signatureless malware prevention
- High-fidelity centralised detection
- Memory protection
- Offline operations (beyond malware prevention)
- On-host storage for offline use cases
- Malicious software
- Hidden artefacts
- Account privilege escalation
- Credential theft

Protect Against:

- Hacktivists
- Insider threats
- State-sponsored attacks
- Organised Crime
- Corporate espionage
- Cyber terrorism
- Kiddie Scripters

What you get

The Team:

- 24/7/365 Real-time monitoring
- 24/7/365 Threat detection and response
- Manned desk 24/7/365
- Team of experienced threat detection experts available via phone and email

The Notifications:

- Critical vulnerability notifications (publicly disclosed vulnerabilities; critical within 48 hours and High within 72 hours)

The Response:

- Proactive managed threat hunting for unknowns on network and endpoints
- Complete managed endpoint threat detection and response service
- Expert investigation of alerts and incidents, and subsequent actions
- Improved forensics and higher-level investigations
- Advanced response capabilities
- Advanced on-host prevention
- Advanced on-host threat hunting
- Improved threat intelligence based on indicators and behaviours captured from global insights

The Understanding:

- Behavioural analytics and network traffic detections
- Platform access to manage your incidents
- Bespoke dashboards for management and technical teams
- Read-only access to our cloud Security Information and Event Management (SIEM)
- Security data collection with data sovereignty (all sorted within the UK boundary)
- Data retention with existing anti-virus or endpoint security solutions
- Dedicated Account Manager
- Digital forensics and incident response (chargeable service with a 5% discount)

Get in touch with a member of the Cyberfort team at info@cyberfortgroup.com, or call 01304 814800.