Arcturus

Part of the CYBERFORT group

Make the trend your own

Choose from two Managed Detect and Response solutions

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

Your MDR will combine human-led investigations, machine learning, real-time monitoring and incident response from a team of cybersecurity specialists from Arcturus, part of the Cyberfort Group. Each solution is built from the ground up for your business – strengthening your security posture wherever it needs it most. And we'll be here all the way as your partners in security.

CYBERFORT

Read on to discover the two levels of MDR you can make your own.

MDR 9 to 5

Monitor the essentials, automate your notifications and speak to an operator during standard business hours, Monday to Friday (09:00–17:30).

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
- Unauthorised software
- Hidden artifacts
- Account privilege escalation
- Credential theft

Protect against:
- Hacktivists
- Insider threats
- State-sponsored attacks
- Organised crime
- Corporate espionage
- Cyber terrorism

What you get

The team:
- 24/7/365 real-time monitoring
- 24/7/365 threat detection and response
- Manned desk during standard business hours (Mon – Fri, 09:00 – 17:30)
- Team of experienced threat detection experts available via phone and email

The notifications:
- Critical vulnerability notifications (publicly disclosed vulnerabilities; critical within 48 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
- Read-only access to our cloud Security Information and Event Management (SIEM)
- Security data collection with data sovereignty (all stored within the UK boundary)
- Data retention to meet your requirements
- Integration with existing anti-virus or endpoint security solutions
- Dedicated Account Manager
- Digital forensics and incident response (chargeable service)

Chosen MDR 9to5 – or want to know more?
Get in touch with a member of the Cyberfort team at **info@cyberfortgroup.com,** or call **+44 (0)1635 015 600.**

MDR 24/7

Get a fully personalised service that includes monitoring of the essentials, automation 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
- Unauthorised software
- Hidden artifacts
- Account privilege escalation
- Credential theft

Protect against:
- Hacktivists
- Insider threats
- State-sponsored attacks
- Organised crime
- Corporate espionage
- Cyber terrorism

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 stored within the UK boundary)
- Data retention to meet your requirements
- Integration with existing anti-virus or endpoint security solutions
- Dedicated Account Manager
- Digital forensics and incident response (chargeable service with a 5% discount)

Chosen MDR 24/7 – or want to know more?
Get in touch with a member of the Cyberfort team
at **info@cyberfortgroup.com,** or call **+44 (0)1635 015 600.**