Managed Detection and Response

ANS

Think Bigger.

Cybersecurity threats aren’t slowing down.

The threat landscape in numbers.

$13.82 trillion
Estimated annual cost of global cybercrime by 2028.

[Source: Statista]

70% of medium-sized businesses have experienced some form of cybersecurity breach in the last year.

[Source: Department for Science, Innovation & Technology]

74% of large businesses have experienced some form of cybersecurity breach in the last year.

[Source: Department for Science, Innovation & Technology]

84% of businesses have suffered a phishing attack.

[Source: Department for Science, Innovation & Technology]

Cybercrime is the world’s **third-largest economy**, after the US and China.

[Source: World Economic Forum]

ANS

Organisations need around-the-clock protection.

In today's threat landscape, businesses of all sizes, industries and sectors are potential targets for cybercrime. However, building a dedicated internal Security Operations Centre (SOC) with the necessary skills, experience and tooling is prohibitively costly and resource intensive:

- Experienced SecOps professionals are in high demand.
- Most providers don't offer true 24/7/365 cover, where incidents of all priority levels are addressed 24 hours a day.
- Security resource is often shared with other IT infrastructure roles.
- Filling internal skills gaps for security specialisms is challenging.
- Attackers are getting more sophisticated – cybercriminals are using AI too.
- The proliferation of the 'Cybercrime-as-a-Service' model has exponentially increased the number of attackers and threats.

What is MDR?

MDR is powered by Microsoft Sentinel, Defender XDR, and our advanced Security Orchestration, Automation & Response (SOAR) platform. It leverages both global and industry-specific threat intelligence to deliver comprehensive protection, taking full responsibility for the security of your multi-cloud environment.

Why ANS?

A partner, not just a supplier

We're an extension of your security team, giving you access not just to the ANS SOC Team, but to your own Customer Success Manager and Customer Success Architect.

Better together

When combined with our Managed Cloud service, MDR offers full Detection, Response and Containment, all the way through to Remediation. We can be your one partner for Security and Managed Service, with domain expertise across Managed Cloud, Data, Business Applications, and more.

A multi-disciplinary approach

Our highly experienced SOC team have access to domain experts across Security, DevOps, Secure Connectivity, Business Apps, Multi-cloud, Data & AI, and more.

Strong partnerships with leading industry providers

Working with industry-leading security partners like Microsoft, VMware, Fortinet and Cisco, we bring our vast experience using modern security tooling to guarantee the safety and security of your hybrid cloud environments.

Full 24/7/365 coverage

Assurance from our entirely UK-based Security Operations Centre covering all incident severity levels 24 hours a day.

A full Find, Tell and Fix service

Not just Find and Tell. We can remediate incidents through our technology specific practices, with industry-leading SLAs.

MDR Features and Components.

Our MDR service comprises best-of-breed security tooling and components supporting experienced human experts:

ANS Security Orchestration, Automation & Response (SOAR) platform

Providing the ability to pre-plan and enact investigation and response actions at machine speed. Governance-led incident closure, with all false positives closed by an Analyst.

Microsoft Sentinel

The industry leading Security Incident and Event Management (SIEM) platform from Microsoft. 300+ out of the box and bespoke integrations ensure a consolidated view and coverage of all major security tooling, from End Point Protection to Firewalls.

ANS Security Operations Centre (SOC) Team

An entirely UK-based, human-operated SOC providing 24/7/365 support and protection.

Microsoft Defender Extended Detection & Response (XDR)

Deploying AI and automation to detect and respond to threats across your whole estate.

Threat Intelligence

Tailored and focussed on your specific industry and organisational area.

Dark Web Monitoring

Detecting and identifying potentially compromised credentials and taking action.

MITRE ATT&CK

Our MDR service makes sure that you are protected and if anybody does try to attack you we can detect it and contain it quickly. ANS use MITRE ATT&CK to assess the coverage of the service, which is a knowledge base of adversary tactics and techniques based on real-world observations.

What's included?

Features	ANS MDR
SOAR	✓
Service Dashboard (ANS Glass)	✓
Managed Defender Tooling	with Managed EDR or XDR
UK-based 24 x 7 x 365 SOC	✓
Incident Containment	✓
End to End Remediation	with other Managed Services
Major Incident Management	✓
Threat Intellgence	✓
Phishing Cover	✓
Managed Microsoft Sentinel	✓
Dark Web Monitoring	with Bolt-On
Threat Hunting (Scheduled)	✓
Non-Defender Log Sources	✓
Service Reviews (CSA + CSM)	✓

Powered by Microsoft Sentinel | Defender XDR | Defender for Cloud | ANS SOAR

MDR Service

Details

- 24 x 7 x 365 Managed SOC
- UK Based
- Managed Microsoft Sentinel
- Detection, Investigation & Containment
- Fully Managed or Co-Managed
- Incident Management
- Monthly reporting
- Scheduled Threat Hunting

Security Tooling

Details

- Fully integrated support of Microsoft Services and Security Stack including Azure, Entra, M365 and Defender
- 400+ Integrations with non-Microsoft Services including Multi-cloud (AWS & GCP)
- Threat Intelligence
- ANS Case Management and Automation

Bolt-on Services

Details

- Attack Surface Management (ASM)
- Security Centre of Excellence (CoE)

Security Team

Details

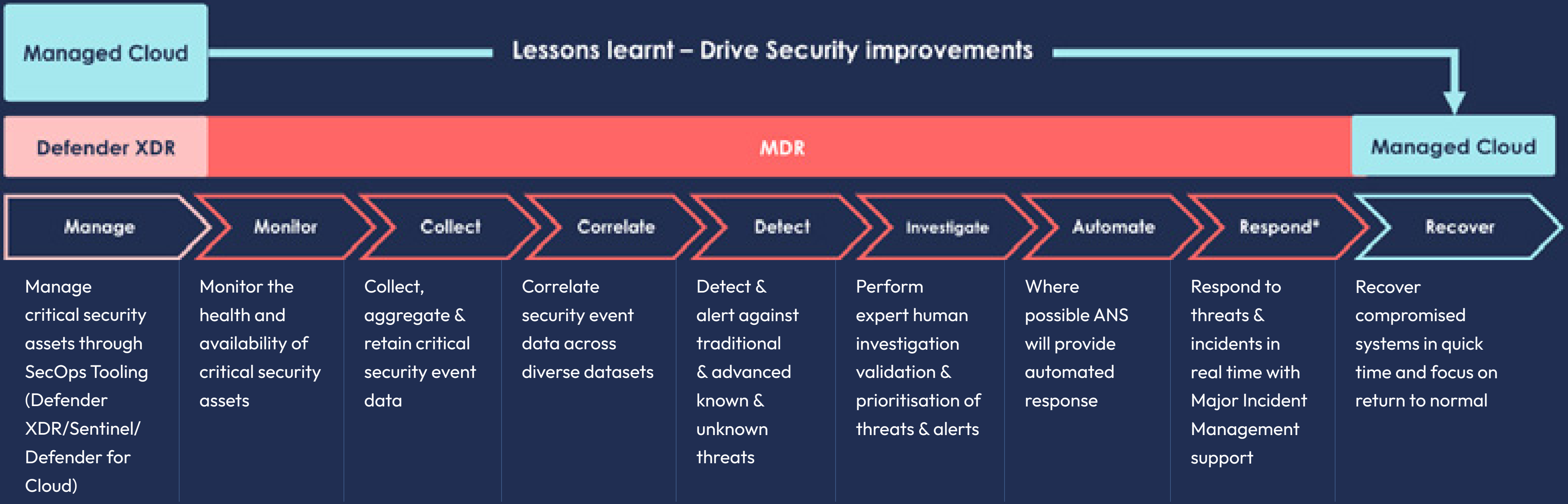
- Security cleared
- Tier 0 – automation and AI
- Tier 1-3 – SOC Analysts
- SecDevOps Engineers
- Threat Hunters
- Customer Success Manager
- Customer Success Architect
- Security Engineers (CoE)

How it works.

The Managed Detection & Response operates along a multi-stage process to ensure that all threats are identified, investigated and contained at rapid pace.

Better Together

When combined with ANS' Managed Cloud and XDR offerings, the MDR process can be augmented with recovery and management capabilities that strengthen your security posture & maturity while decreasing cost.



Manage critical security assets through SecOps Tooling (Defender XDR/Sentinel/ Defender for Cloud)

Monitor the health and availability of critical security assets

Collect, aggregate & retain critical security event data

Correlate security event data across diverse datasets

Detect & alert against traditional & advanced known & unknown threats

Perform expert human investigation validation & prioritisation of threats & alerts

Where possible ANS will provide automated response

Respond to threats & incidents in real time with Major Incident Management support

Recover compromised systems in quick time and focus on return to normal

Combined Major Incident response teams consisting of cloud, security and data engineers.

Single Point of Contact for Major Incidents and will be managed via our ANS war room with all relevant teams.

24/7/365 service.

Drive and manage Security posture access Azure and Endpoints.

Full transparency of the service.

*Customer will be responsible for actions outside the scope of ANS services

ANS

What are the benefits?

With ANS MDR, your organisation will:

- Minimise risk from security threats.
- Receive full 24/7/365 protection against attacks, for all incident severities.
- Free up resource to allow your team to focus on other priorities.
- Cost-effectively augment existing cybersecurity capabilities.
- Requirements for regulatory compliance and cyber insurance to meet SIEM and SOC mandates.
- Benefit from multi-disciplinary security experts across Multi-Cloud, Data, Connectivity, Business Apps and more.
- Achieve optimal results from our service with the help of our dedicated Customer Success function.

ANS

How we engage.

Navigators

A Navigator provides a strategic assessment of your current and future state.

Detect & Respose Navigator

We'll assess your organisation's ability to plan, prepare, detect, contain, and recover from cyberattacks. Through a combination of questionnaires and security workshops, it identifies gaps and strengths in your current approach, delivering a detailed report and actionable recommendations to enhance your cyber resilience.

Sentinel & Defender for Cloud Check Navigator

We'll ensure your Microsoft Sentinel and Defender for Cloud platforms are optimised and configured to Microsoft best practices. It includes a thorough review, security workshops with ANS architects, and a detailed report with recommendations to enhance your security operations and drive efficiency.

Envisioning Workshops

Our Envisioning Workshops involve the deployment of essential tools and techniques. You may be eligible for a funded workshop.

Threat Protection Workshop

Learn how Microsoft 365 Defender, Defender for Cloud, and Microsoft Sentinel work together, enabling you to adopt a modern XDR approach for your endpoints and workloads.

Cloud Security Workshop

We'll assess your security landscape and address your most pressing security goals and challenges, providing an immersive experience that brings the Microsoft security vision and capabilities to life.

Modern SecOps Workshop

This Workshop is focused on the Microsoft Sentinel technology and best practice architecture, creating a foundation for you to fully adopt a SecOps process through all your infrastructure at cloud scale.

Data Security Workshop

The Data Security Workshop is designed to create customer intent for deploying and adopting Microsoft Purview solutions by providing real data driven examples of data security and regulatory risks in your own environments.

One of the most highly certified security partners in the UK.

ISO

- ISO 14001:2015 Environmental management
- ISO/IEC 27001:2013 Information security management
- ISO 9001:2015 Quality management
- ISO 22301:2019 Security and resilience
- ISO/IEC 27017:2015 Security techniques
- ISO/IEC 27018:2019 Security techniques
- ISO/IEC 20000-1:2018 Information technology
- UKAS ISO/IEC 42001 certification

Member of Microsoft Intelligent Security Association
Microsoft

Mandiant

GROUP-IB

LogicMonitor

CYBER CROWD

VIRUSTOTAL

Symantec. by Broadcom

Carbon Black. by Broadcom

ARROW

Microsoft
2024 UK Partner of the Year Awards
UK Services

Microsoft Partner
Azure Expert MSP
Microsoft

Microsoft
Solutions Partner
Microsoft Cloud

Microsoft
Solutions Partner
Private Cloud

Microsoft
Solutions Partner
Infrastructure
Azure
Specialist
Infra and Database Migration
Azure VMware Services
Azure Virtual Desktop

Member of
Microsoft Intelligent Security Association
Microsoft Security
Microsoft Verified Managed XDR Solution

Microsoft
Solutions Partner
Security
Specialist
Copilot
Cloud Security
Threat Protection

25|26
INNER CIRCLE

Microsoft
Solutions Partner
Business Applications
Specialist
Copilot
Low Code Application Development

Microsoft
Solutions Partner
Data & AI
Azure
Specialist
Infra and Database Migration
Analytics
Build AI Apps on Microsoft Azure

Microsoft Fabric
Featured Partner

Microsoft Fabric
Databases
Featured Partner

Microsoft
Solutions Partner
Digital & App Innovation
Specialist
Low Code Application Development

Microsoft
Solutions Partner
Digital & App Innovation
Azure
Specialist
Build AI Apps on Microsoft Azure

Microsoft
Solutions Partner
Modern Work
Specialist
Copilot

Microsoft
Copilot Jumpstart Partner
Prioritized Tier

Microsoft
FastTrack
Partner

ANS

Get in touch.

Telephone
0800 458 4545

Web
www.ans.co.uk

Address
ANS Group
Birley Fields
Manchester
M15 5QJ

ANS Think Bigger.