Managed detection and response

Powered by Microsoft Sentinel

ANS Think Bigger.

Contents.

05 Your managed service

06 Microsoft Sentinel

07 Threat detection and response

09 Incident management and SLAs

11 Use case management

12 Service roles and responsibilities

13 Sentinel management and integration

14 SOAR

16 Service management and SecOps

17 Customer Success Manager

18 Reporting

19 Customer Success Architect

20 ANS Glass

21 Virtual CISO service

22 Center of Excellence

23 Additional services

25 How we engage

MCR. 1996

Over 25 years experience

Dedicated agile squads

NPS score of 85+ on average

ISO expert credentials

24/7/365 support and SOC

400 first-class tech experts

200 Apprentice graduates from our 'Outstanding' Academy.

Celebrating our differences

- Cloud & Infrastructure
- Modern Work
- Security & Connectivity
- Digital & App Innovation
- Data & AI
- Business Applications

Over 1000 Vendor certifications.

Gold Microsoft Partner
Azure Expert MSP
Microsoft

One of the most highly certified partners in the UK.

Gold
Microsoft Partner
Azure Expert MSP
Microsoft

Advanced Specialisation
Cloud Security

Advanced Specialisation
Analytics on Microsoft Azure

Advanced Specialisation
Windows Server & SQL Server
Migration to Microsoft Azure

Member of Microsoft Intelligent
Security Association

Microsoft Partner of the
Year Finalist 2020 & 2021

Gold Cloud Business
Applications

Gold Security

Gold Cloud Platform

Gold Data Analytics

Gold Data Platform

Gold Application
Development

Gold Application
Integration

Gold DevOps

Gold Small & Midmarket
Cloud Solutions

Gold Datacenter

Gold Windows & Devices

Gold Cloud Productivity

Gold Collaboration and Content

Gold Messaging

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

Welcome to your Managed Service.

Our Managed Services are designed to empower you with the knowledge and education to drive improvements, the platforms and tools to gain real-time insights and a dedicated customer success architect to help you achieve continuous optimisation and development of your environment.

Knowledge

- High touch service management
- Customer success manager to drive improvements

Education

- Dedicated expertise
- Customer Success Architect (CSA) to ensure technical excellence

Efficiency

- End to end platfrom operations
- Operational tooling including LogicMonitor, CloudHealth and Sentinel as standard

Governance

- Financial insights
- Security operations
- Continued optimisation and development through scheduled CSA reviews

Visibility

- Continued real time insights and education through our bespoke management tool, Glass.

Microsoft Sentinel.

We'll take complete responsibility for the availability and performance of your Sentinel environment as well as the response and investigation of alerts generated by the platform.

Unlike most MSPs, which just identify, investigate, and provide guidance on remediation, ANS is uniquely positioned to actively remediate incidents on your behalf. To benefit from this, you will need to have an additional contract such as Managed Cloud which will enable us to remediate incidents under change control.

Our Managed Detection and Response service operates across 3 key domains

- Threat Detection and Response
- Sentinel Management and Integration
- Service Management and SecOps

Each domain provides several core services to increase technical and operational efficiency so you can focus on innovation and driving your business forward, while ANS focus on optimising your security environment.

Threat Detection and Response.

Threat Detection and Response provides 24/7/365 proactive support giving you the reassurance that ANS and Microsoft are working together to provide high touch support on your business-critical Sentinel environment.

Security advice and incident remediation

Our Managed Detection and Response service will give you access to certified security analysts who will provide hands on advice and support of your Sentinel environment.

The service enables us to

- Provide data, interpretation, and remediation advice for incident response and security incidents
- Provide advice on how to contain and remediate security incidents*
- Monitor the platform to provide bespoke workflows, thresholds, availability and performance

*If ANS is providing you with a managed service for the underlying platform, we will remediate any incidents on your behalf.

Platform availability and real time monitoring

Using Logic Monitor, ANS will ensure Sentinel is always available and operational.

The intelligent platform leverages tagging to provide flexible escalation workflows within the ANS proactive support process, allowing for dynamic actions based on individual services. For example, resources tagged 9X5 would automatically stop raising alerts outside of the working hours, reducing the overnight burden of actioning unnecessary alerts.

Logic Monitor will provide

- Azure Log Forwarder VM monitoring
- Connectors
- Log Analytics workspace
- Source Technology (where ANS supported under another Managed Service e.g. Managed Cloud)

Incident management and SLAs.

Our architecture validation and design guidance is delivered in line with a defined service level agreement (SLA).

Our 24/7/365 proactive support provides you with

- Round the clock event management and alert triaging directly from our Secure Operations Centre
- End-to-end incident management with financially backed SLAs for a fast and effective resolution
- Dynamic escalation paths for smooth integration with your existing team, processes and rotas

Incident priority	Threat severity rating	Response SLA	Escalation notification	Notification type
P1	Critical	30 mins	Immediate	Phone call
P2	High	1 hour	None	Email/Glass
P3	Medium	4 hours	None	Email/Glass
P4	Low	1 day	None	N/A
P5	Question Query	2 days	None	N/A

Priority escalation to Azure Sentinel for faults

We will provide priority escalation to Microsoft Premier Support for Azure Sentinel Platform issues.

High priority escalation to vendor

We will provide high priority escalation to Microsoft Premier support for P1 business critical faults relating to the Azure Sentinel Platform.

Threat Severity Ratings

A security incident is a pattern of potentially malicious activity that implies a threat to an information system, violates acceptable use policies, or circumvents standard security practices.

ANS classifies incidents into four threat severity ratings: Critical, High, Medium, and Low.

Incident priority	Threat severity rating
P1	Critical
P2	High
P3	Medium
P4	Low

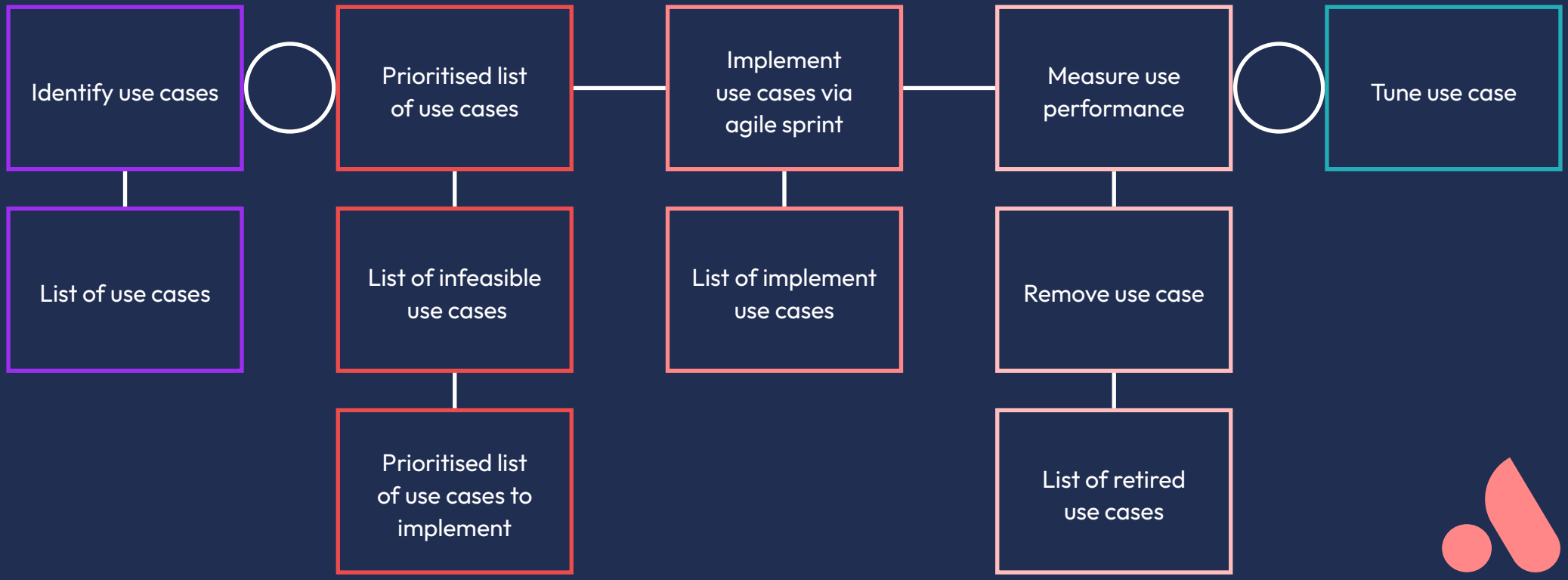
There are 4 methods for engaging with ANS for technical support

- ANS Glass portal
- Microsoft Teams
- Phone
- Email

Use case management.

We have industry specific use-cases spanning public and private sectors. Our COE team will build specific uses case for industries to protect business critical assets and functions.

- Gartner aligned modern use case management
- Agile process for deploying use cases for security management, with glossary of common use cases
- Statement of work is based around use cases and the type of responses required for each case
- Use cases drive modern tooling configuration
- Lifecycle to be managed by COE with addition and retiring of use cases on an ongoing basis



Services, roles and responsibilities.

The following RACI Matrix details the responsibilities of both ANS and the customer within the Managed Detection & Response service.

R: Responsible | A: Accountable | C: Consulted | I: Informed

Activities	ANS				Customer			
	R	A	C	I	R	A	C	I
Data connector configuration	•	•					•	•
Standard workbook configuration	•	•					•	•
Platform monitoring	•	•					•	•
Incident and change management - platform	•	•					•	•
Incident and change management - security alerts	•	•					•	•
Log forwarder VM deployment - Azure	•	•					•	•
Log forwarder VM deployment - on premise (unless relevant ANS MS in place)			•	•	•	•		
Configuration of customisation of Sentinel detection rules								
Configuration of cource technology sending logs into Azure Sentinel (unless relevant ANS MS in place)								
Creation of hunting queries	•	•					•	•
Creation of hunger queries in jupyter notebooks			•	•	•	•		
Creation of Azure sentinel playbooks to automate threat response								

Sentinel management and integration.

Our team of Sentinel platform experts will continually manage, maintain and optimise your platform. We will ensure any integration with your infrastructure, or your IT service is developed and managed to give you a comprehensive security capability as well as ensuring it's maintained moving forwards. Once your platform is up and running, we'll continue to fine tune your Sentinel environment to make sure the platform is always automated and orchestrated to best practice.

As part of this service, we will configure

Data connectors
We'll configure and deploy specified connectors in Azure as requested by you.

Workbooks
On request of a connector, we'll configure available workbooks to enable you to monitor the insights from the data connectors.

Notebook and maintenance
We'll create and maintain notebooks used for bespoke threat hunting.

Tailored alert tuning
We'll regularly tune Sentinel alerts tailored to your requirements to remove noise/minimise false positives and reduce consumption costs.

Log forwarder deployment
You will be required to deploy and configure new Log Forwarder VMs as required with support from ANS.

Custom workbooks
If you have configured connectors from scratch to create custom insights, we will create custom workbooks for you.

Playbook and maintenance
we'll create and maintain Playbooks* used for SOAR, and you will receive access to ANS' maintained catalogue of workbooks.

Detection rules
we will configure and customise Sentinel detection rules in line with your requirements.

What are playbooks?

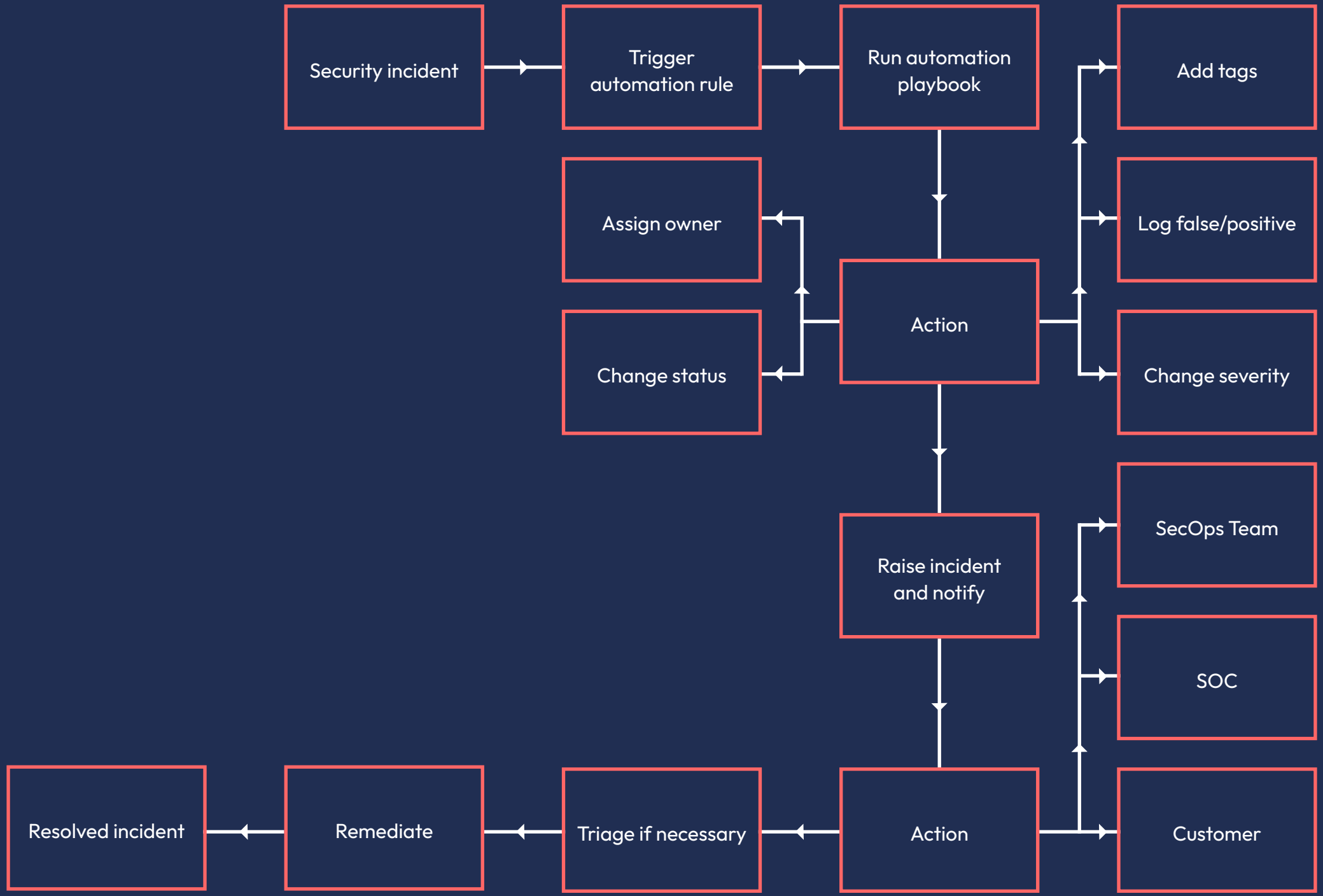
Collections of procedures that can be run from Microsoft Sentinel in response to an alert or incident. It can help automate and orchestrate responses and can be set to run automatically when specific alerts are generated by being attached to an analytics rule or an automation rule, respectively.

Security Orchestration and Automated Response (SOAR)

When a security incident occurs, it will trigger an automation rule in Sentinel. These rules are configured and managed by the ANS Managed Detection and Response service.

Once this trigger is activated, it invokes a Sentinel Playbook (Automation script/Logic App) that will produce a series of configurable actions. These actions will be assigned an owner (such as a subject matter expert or analyst) who will change the status of the incident along with the severity depending on the incident risk profile. It will then be logged as false/positive in order to update the AI/ML for future triggered incidents of the same nature.

This will automatically raise an incident in ANS Glass and/or your ITSM depending on security severity. If triage is necessary, this incident will be triaged by the ANS SOC, then passed to the ANS SecOps analyst or specialist to record and remediate the incident. Once this has been completed, the incident is logged and recorded as resolved.


Security incident
Trigger automation rule
Run automation playbook
Add tags
Assign owner
Log false/positive
Action
Change status
Change severity
Raise incident and notify
SecOps Team
SOC
Resolved incident
Remediate
Triage if necessary
Action
Customer

Service management and SecOps.

Drive improvements across Microsoft Sentinel

Built upon industry leading tools and processes, ANS' Service Management is designed to enable you to maximise the value of your Microsoft Sentinel investment.

Customer Success Manager.

Your Customer Success Manager will ensure you receive continual service improvements across your Managed Detection and Response service.

Continuous service improvement is designed to align our services with your changing business needs by identifying and implementing improvements to those services to support. This ensures that processes, practices and services are continually reviewed, and any lessons learned introduced as improvements, such as devolving further task automation workflows.

The core objectives of continual service improvement include

- Action security incidents, events and changes
- Monitor and track key information about your security platform
- Monitor your Azure Sentinel environment including month to date spend in real time, billing history and cost savings
- View specific date information such as scheduled security changes and SecOps consultant days in the calendar view
- Access transparent and detailed SecOps contractual information
- View security recommendations as well as current and previous scores on a month by month basis

Reporting.

Each month, your Customer Success Manager will lead a Service Management Review (SMR) to provide you with in-depth reporting on your Managed Detection & Response service.

They'll provide you with insights on the trends and analysis they have uncovered as well as reports on efficiency and optimisation. This includes proactive monitoring of your Sentinel environment so we can align our services to your changing business needs as they happen.

Your monthly SMR will include

- An executive summary of the highs and lows of your service
- Cost efficiencies, including potential savings and costs per application in the cloud
- A report of incidents, changes and problems raised and how they were met in line with agreed SLAs
- The status of current projects and any due renewals

Sentinel Reporting

In addition to the standard SMR content listed, you will also receive specific Sentinel reporting on the following:

Data collection health

We'll cover:

- Newly deployed connectors
- Any storage issues
- Retention policies
- Trends from the previous month

Connector Workbook Data

We'll cover:

- Trends
- Connectors driving the majority of events
- Your internal response process to find out what is working well, any challenges and where ANS can support improvements
- ANS best practices based on delivering Threat Management
- Threat hunting and analytics
- Relevance and cost review

Please note reporting will differ slightly based on which connectors and workbooks are in place.

Customer Success Architect.

As an ANS customer, you'll receive a dedicated Customer Success Architect (CSA).

Your dedicated CSA will understand your organisation and your IT environment and will use this deep understanding to help drive the maturity of your team and execute on your strategic roadmap. Your CSA will review your security health on a regular basis to make sure your environment is always optimised and you're making the most of Microsoft Sentinel.

Your CSA and our team of technical experts will also use a number of bespoke systems and in-house skills which can add a further layer of operational excellence to your Sentinel solution.

These include

- Regular pro-active security monitoring with an Enterprise Grade Monitoring Platform
- Analysis and recommendations for security posture improvements
- Discovery opportunities to streamline and tune Sentinel environment
- Well-architected peer review and guidance for security initiatives
- Enablement of relevant modern security and platform technologies
- Hybrid cloud security architectural and governance advice

Your CSA will also help you to

- Improve Sentinel platform efficiency
- Identify opportunities to improve your Sentinel service
- Define standards and best practices for the management of new technologies
- Provide technical analysis and support

ANS Glass.

Using Glass, our real-time service management portal, you'll receive a transparent, single view of all service transactions.

Glass works by surfacing information from industry leading tools into a centralised portal so you can rest assured your Sentinel environment is operating as efficiently as possible. From incidents and changes to contractual information and reporting, the digital interface provides anytime, anywhere access. Developed using feedback from our customers, Glass is much more than a traditional ticketing system. The portal offers a digital and efficient way for you to communicate any requests or notifications with ANS, allowing you to do the following:

- Action incidents and changes
- Monitor key information about your live projects
- Access transparent and detailed contract information
- Monitor your environment including month to date spend in real time and cost saving
- View specific date information such as scheduled changes in the calendar view
- Provide recommendations as well as current and previous scores on a monthly basis

Virtual CISO service.

Benefit from board-level expertise across the cyber security domain As well as being paired with a dedicated Customer Success Manager and Customer Success Architect, you can also choose to benefit from our virtual CISO (vCISO) service*.

Our vCISO will ensure your security posture strengthens over time. Whether implementing controls to meet compliance regulations, or to identify areas of weakness through a gap analysis. Our vCISO service works in an agile methodology to ensure continual improvement through regular workshops and consultancy sessions to fit your needs.

Their key responsibilities will include

- Conducting gap analysis assessments against frameworks and standards
- Conducting security posture analysis against targeted areas
- Running regular sessions to ensure key objectives are met
- Providing security reporting for board level management
- Providing scenario based testing against incidents
- The production of policy sets bespoke to your organisation
- The production of risk assessment and modelling
- Identifying technical controls to improve security posture

What you'll gain from this service

- Higher level of security assurance for internal and external stakeholders
- Validation of your controls completed by an experienced s ecurity consultant
- More effective management of Data Breaches and/or Cyber Security Incidents
- Pragmatic and cost-effective support, ensuring maximum ROI
- Cyber Security policies that support your organisation
- The ability to make informed, risk-based decisions
- Access to technical skills and resources, allowing continuous improvement
- Support in the attainment of certifications
- National Security Vetted personnel

*Please note that this service incurs an additional cost.

Centre of Excellence (CoE)

ANS' Centre of Excellence is designed to give you the ability to tap into a rich pool of skills and resources as and when you need them, without the burden of having to build your own in-house capability. This means you avoid paying for expensive resource in-house that you may not need all year round.

Through COE, you can add additional functionality to Managed Detection and Response, and SOC with:

- Customer SOAR playbooks
- Advanced use case management

This is to be delivered at an hourly rate with "SOC COE' credits.

- Data source management
- Detection reduction rule implementation

SOC COE Remediation Packages from CSA/CISO functions (30,60 & 90 Hour packages per PCM).

- Threat hunting notebooks
- Remediation and optimisation

Drive to build the use case model to using an agile methodology.

Additional services.

Managed XDR

Our Managed XDR service is a subset of our MDR service which enables us to manage your endpoint and workload protection assets using the Microsoft XDR products of Microsoft Sentinel, M365 Defender & Defender for Cloud.

Managed SASE/SDWAN

Our Secure SDWAN services is fully integrated into our MDR services using Microsoft, Fortinet and Cisco tooling with technology specific use cases associated to our customers connectivity requirements.

Managed Firewall

Managed Firewall provides proactive management of your cloud hosted Firewalls removing the administrative overhead on IT operations to ensure your systems remain compliant and secure.

Managed Patching

Managed Patching provides proactive management of your patching requirements removing the administrative overhead on IT operations to ensure your systems remain compliant and secure.

Managed Back Up/DR

This Backup and restore service will give you an Enterprise Level Backup solution, access to Commvault and Azure qualified experts and Proactive Management and Testing of Restore capabilities throughout the service lifetime.

Managed Cloud

Managed cloud is designed to enable you to maximise the value you receive from your public cloud investment. Our UK-based advisory services, technical expertise, governance management and reporting will increase operational value, whilst our financial insights and automation reduce your platform consumption

How we engage.

Our security operations formula is designed to help you to overcome the complexities of modernising your security operations while working with you to build the business case and roadmap for migrating to a modern SecOps environment. We'll then accelerate your adoption of Microsoft Sentinel before onboarding you into our high-touch managed service.

SecOps Navigator

Our SecOps Navigator service enables us to take a strategic look at your security operations. We'll establish 'where you are now' and understand 'where you need to go' to deliver on your strategic objectives. We'll then build a high-level transition plan detailing how you move from your existing estate to your future vision and the cost of the change in order to provide you with a quantifiable business case supporting your security operations initiative.

Microsoft Sentinel Accelerator

Once you've completed the SecOps Navigator, we can help you adopt Microsoft Sentinel at pace. This Accelerator is high-value, low-cost solution which can be delivered in as little as 6 weeks, making this an ideal if you're on a tight deadline.

Using our unique Accelerator approach to delivery enables you to benefit from:

- A fully extendable solution
- High touch project support
- Rapid time to value
- Proven architecture provisioned with demonstrated success

Want to know more?

To find out more about our service offerings, please reach out to your Account Manager or...

Visit ans.co.uk →

Get in touch.

Telephone
0800 458 4545

Web
www.ans.co.uk

Address
ANS Group
ANS Campus
Birley Fields
Manchester
M15 5QJ

ANS Think Bigger.