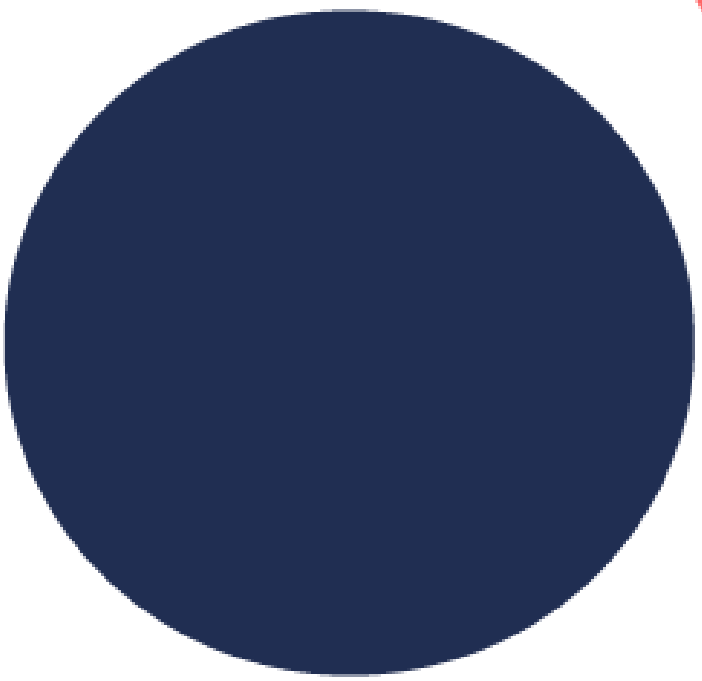
Modern SecOps Workshop

Statement of Work

For [CUSTOMER]



Contents

ANS
One Archway
Birley Fields
Manchester, M15 5QJ
0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk
Co. Reg No. 3176761
VAT No. 245684676

Notice

One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676

ISO Document Control

Document Control	
Document Name	Modern SecOps Workshop Statement of Work for [CUSTOMER]
Date Originated	14/08/25
Status	V1.0
Document Author	
Document Owner	
Approved by	
SOW Valid Until	4 weeks from issue date

Version Control	
Version Stage	New Document
Document Creation	14/08/25
v1.0 Issue Date	14/08/25

Document Team			
Name	**Role**	**Telephone**	**E-mail**
AM/AE			

Document Distribution			
Name	**Role**	**Telephone**	**E-mail**
Customer	Details	Here	And here
Customer	Details	Here	And here

One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676

1. Purpose

The purpose of this document is to outline the key deliverables required to design and implement Microsoft Sentinel within the [CUSTOMER] tenant as part of a Microsoft Sentinel Workshop engagement.

This is Workshop delivered free of charge on the assumption that [CUSTOMER] has been approved for funding by Microsoft and ANS are allowed to share Proof of Execution (PoE) to Microsoft to qualify the funding following delivery.

This document demonstrates ANS capability as a leading Microsoft Cloud & Security Services Provider, to deliver a Sentinel Proof of Concept.

ANS understands that [CUSTOMER] is looking to bolster their wider security posture and have identified Sentinel as a tool for detecting, investigating, and responding to cyber threats. ANS will deliver a fully functioning Microsoft Sentinel platform ready for data to be ingested and interpreted. This includes identities, security, connectors, monitoring, auditing & logging.

1.1 [CUSTOMER] Overview

AM/AE to complete – info about customer, what they do and why they want/need this workshop.

1.2 [CUSTOMER] Contact details

The contact details below will be the initial contact point for ANS during the deployment of the Sentinel Accelerator.

Name	Role	Email	Telephone
Details			
Details			

1.3 Engagement Type

This document is the statement of work to onboard customer to the MDR service, at a high level it includes.

- Implementation of a single Sentinel instance in [CUSTOMER] tenant.

1.4 Document Scope

This document will cover the following:

- High level deliverables.
- Delivery process.
- Deliverables & Prerequisites.
- Deployment model.
- Permissions.
- This document can be considered to be the High Level Design (HLD) for this deployment.

1.5 Deployment Scope

[CUSTOMER] require a new Sentinel deployment as part of this Workshop, and the deployment scope includes:

Microsoft Defender XDR Deployment:

One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676

    - Deploy Trial Licences:
        - Deploy Microsoft 365 for SCI Partner Engagements trial licenses
    - Onboard and confirm Defender XDR service is on.
- Microsoft Entra ID Protection:
    - Verify Microsoft Entra ID Protection is available in Azure Portal.

Sentinel Deployment

- Create a new subscription.
- Create resource group.
- Create Log Analytics workspace (free 30 days log ingestion (if eligible) will commence as soon as the first logs are ingested).
- Enable Microsoft Sentinel on top of the workspace.
- Set workspace retention, daily cap and commitment tiers.
- Deploy the following complete solutions from the Content Hub:
    - Microsoft Defender XDR - Solution
        - Connector must be enabled
        - 5 High rules need to be enabled
    - Microsoft Entra ID Solution
        - Connector must be enabled
            - Must Include Sign in and Audit logs
        - 5 High rules need to be enabled
    - Microsoft 365 Solution
        - Connector must be enabled
            - Must include O365,Exchange Online , SharePoint & OneDrive
    - Azure Activity Solution
    - Microsoft Defender Threat Intelligence
        - Select IOC Sources - ALL is recommended
- Connect Sentinel Workspace to Defender XDR Unified Portal.
- Verify that the following additional workbooks are installed if not install them from the content hub
    - Workspace Usage
    - Sentinel Cost
    - Sentinel Cost Optimization
    - Security Operations Efficiency
    - Data collection health monitoring
- Enable up to 5 Analytic rules per connector
    - Microsoft Defender XDR
    - Microsoft Entra ID Solution
    - Microsoft 365 Solution
    - Azure Activity Solution
    - Microsoft Defender Threat Intelligence

1.6 Not in scope

The following elements are not in scope of ANS delivery for this Statement of Work:

- Any ANS SOC Managed Services. This is only available if the ANS MDR service is being procured.
- Any other design documentation other than this SOW.
- Azure Arc Design, Consultancy or Deployment.
- AMA Agent Design, Consultancy or Deployment.

ANS
One Archway
Birley Fields
Manchester, M15 5QJ
0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk
Co. Reg No. 3176761
VAT No. 245684676

- Log Forwarder Design, Consultancy or Deployment.
- Configuration of endpoints, servers, firewalls, and other network appliances to send data to Sentinel.
- Connectors not listed above; [CUSTOMER] can choose to implement these themselves.
- Workbooks not listed above; [CUSTOMER] can choose to implement this themselves.
- Microsoft Sentinel Hunts, [CUSTOMER] can choose to implement this themselves.
- Any ITSM integration.
- Threat Intelligence integration not listed above.
- Automation and/or playbooks not listed above.
- Production of any other documentation not already defined in this SOW.
- All other work not specifically mentioned in this SOW.

1.7 Document validity

Due to the ever-changing nature of the cloud, this statement of works has a validity date shown below, If the Statement of Works is not reviewed and signed by [CUSTOMER] this date, ANS will need to review the Statement of Works and may need to issue a new one. This is to ensure that [CUSTOMER] requirements align to the latest Microsoft Sentinel services.

[date] (28 days from issue).

1.8 Funding

[CUSTOMER] is eligible for Microsoft funding as part of workshop however it will be the [CUSTOMER]'s responsibility to complete a Security questionnaire before the commencement of this work and complete a customer feedback questionnaire at the end of the workshop to qualify for the funding.

If [CUSTOMER] does not complete the feedback questionnaire within the allotted time then the [CUSTOMER] will be invoiced for work undertaken by ANS.

One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676

2. Deployment

2.1 Delivery Process

The following delivery process will be used to deploy the tooling for the Microsoft Sentinel Workshop.

- **Presales (This will be Completed prior to the SOW being issued)**
  - Completion of questionnaire
  - Prerequisites.

- **Phase 1: Prerequisites**
  - Pre-Delivery Workshop (PDW).
  - Create local security reader account for security review.
  - Create local administration accounts for ANS Engineer.
  - Deploy M365 Trial Licences.
  - Partner Admin Link (PAL).

- **Phase 2: Delivery**
  - Defender XDR Onboarding.
  - Sentinel Deployment:
    - Create 1 x new Subscription.
    - Create 1 x resource group.
    - Create 1 x Log Analytics Workspace.
    - Enable Microsoft Sentinel on top of the workspace.
    - Set workspace retention, daily cap and commitment tiers.
    - Enable health diagnostics for Analytics Rules, Data Connectors and Automation Rules.
    - Deploy the following **complete** Content Hub Solutions to Sentinel.
      - Microsoft Defender XDR
      - Microsoft Entra
      - Microsoft 365
      - Azure Activity
      - Microsoft Defender Threat Intelligence.
    - Onboard to Unified SecOps Portal.
    - Deploy Workbooks including those required for Sentinel Cost Optimisation.

- **Phase 3: Handover**
  - ANS and [CUSTOMER] Sentinel Accelerator Handover workshop.

- **Phase 4: End of Workshop**
  - After 1 month of Sentinel ingesting logs the Microsoft Sentinel Workshop will be completed.
  - ANS and [CUSTOMER] Feedback session
  - ANS and [CUSTOMER] Next Steps Discussion with ANS Account Manage/Executive and Pre-Sales.

2.2 Deliverables and Prerequisites

This section contains a high-level overview of the deliverables, who is responsible for delivering them and what the delivery method will be.

ANS
One Archway
Birley Fields
Manchester, M15 5QJ
0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk
Co. Reg No. 3176761
VAT No. 245684676

This section also covers all the prerequisites that need to be completed by [CUSTOMER] and/or by ANS before Sentinel can be deployed. This section will also clarify the area of responsibility for delivering the prerequisites.

2.2.1 Deployment Prerequisites

Prerequisites - Accounts and Permissions					
Deliverable	**Qty**	**Delivered by**	**Phase**	**Dependencies**	**Comments**
Completion of questionnaire	1	Customer	Phase1: Prerequisites		
Azure Tenant and Azure Landing Zone in Place	1	Customer	Phase1: Prerequisites	Completion of questionnaire	Must be in place or this Workshop cannot start.
Creation of a suitable security subscription or other subscription suitable for Sentinel	1	Customer	Phase1: Prerequisites	Completion of questionnaire	
Customer to review permissions required for both [CUSTOMER] and ANS	1	Customer	Phase1: Prerequisites	Completion of questionnaire	See 2.3
Create local security reader account for security review	1	Customer	Phase1: Prerequisites	Completion of questionnaire	To enable ANS to review [CUSTOMER] environment.
Customer to provide any PIM/Identity Governance requirements before implementation	1	Customer	Phase1: Prerequisites	Completion of questionnaire	To ensure conforms to customer identity governance.
Create Entra administration accounts for ANS Engineer	1	Customer	Phase1: Prerequisites	Completion of questionnaire	Accounts required for implementation can be found in **See 2.3**
Create Entra Security Reader account for ANS Pre-Sales Review	1	Customer	Phase1: Prerequisites	Completion of questionnaire	Local Security Reader account needs to be created in order for ANS to review Sentinel. **See 2.3**
Providing subscription, Azure tenant IDS for [CUSTOMER] environment	1	Customer	Phase1: Prerequisites	Completion of questionnaire	
Prerequisites - Licences					
Correct licences Trial Licences for the Workshop are deployed: • Microsoft 365 E3 (no Teams) for SCI Partner Engagements trial license. • Microsoft 365 E5 Security for SCI Partner Engagements trial license.	1	Customer	Phase1: Prerequisites	-	Only deploy the licences at the start of the workshop. Do not assign these licences to any users.
Prerequisites - Partner Admin Link (PAL)					
Partner Admin Link (PAL) Setup	1	ANS & Customer	Phase1: Prerequisites	-	Please refer to Section 4 for more information about PAL.

One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676

2.2.2 Delivery and Handover

Delivery – Defender XDR					
Deliverable	**Qty**	**Delivered by**	**Phase**	**Dependencies**	**Comments**
Onboard Defender XDR and/or verify Defender XDR Service is on. The following will be visible in the Defender Portal: • Incidents management • Alerts queue • An action centre for managing automated investigation and response • Advanced hunting capabilities • Threat analytics	1	ANS or Customer	Phase 2: Delivery	Phase 1 - Pre-Reqs - Licences	Defender XDR may have already been onboarded, if so verify the Defender XDR service is enabled .

Delivery – Microsoft Entra ID Protection					
Deliverable	**Qty**	**Delivered by**	**Phase**	**Dependencies**	**Comments**
Verify Microsoft Entra ID Protection Blade in Azure Portal is accessible.	1	ANS or Customer	Phase 2: Delivery	Phase 1 - Pre-Reqs - Licences	Entra ID Protection may have already been onboarded, if so verify the service can be accessed.

Delivery - Microsoft Sentinel					
Deliverable	**Qty**	**Delivered by**	**Phase**	**Dependencies**	**Comments**
This completed SOW will act as a high-level design for this deployment.	1	ANS	Phase 2: Delivery		
Creation of new Subscription	1	Customer and ANS	Phase 2: Delivery	Phase1: Prerequisites	
Creation of log analytics workspace	1	ANS	Phase 2: Delivery	Phase1: Prerequisites	
Implementation of Microsoft Sentinel in X Azure Region	1	ANS	Phase 2: Delivery	Phase1: Prerequisites	
Deploy content hub solution for Microsoft Defender XDR: • Add content from Content Hub. • Configure Data Connector. • Threat Analytics rules are not required in Sentinel as Unified Portal will deal with this. • No Workbooks to be deployed.	1	ANS	Phase 2: Delivery	Phase1: Prerequisites	See 0
Deploy content hub solution for Entra ID: • Add content from Content Hub. • Configure Data Connector: ○ Sign-on and Audit logs only. • Enable out-of-the-box threat analytics rules using default values. • Deploy Workbooks:	1	ANS	Phase 2: Delivery	Phase1: Prerequisites	See 0

ANS
One Archway
Birley Fields
Manchester, M15 5QJ
0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk
Co. Reg No. 3176761
VAT No. 245684676

Delivery - Microsoft Sentinel					
Deliverable	**Qty**	**Delivered by**	**Phase**	**Dependencies**	**Comments**
○ Microsoft Entra ID Sign-in logs. ○ Microsoft Entra ID Audit logs.					
Deploy content hub solution for Microsoft 365: • Add content from Content Hub. • Configure Data Connector. • Enable out-of-the-box threat analytics rules using default values. • Deploy Workbooks: ○ Office 365 ○ Exchange Online ○ SharePoint & OneDrive	1	ANS	Phase 2: Delivery	Phase1: Prerequisites	See 0
Deploy content hub solution for Azure Activity: • Add content from Content Hub. • Configure Data Connector. • Enable out-of-the-box threat analytics rules using default values. • Deploy Workbook: ○ Azure Activity	1	ANS	Phase 2: Delivery	Phase1: Prerequisites	See 0
Deploy content hub solution for Defender Threat Intelligence: • Add content from Content Hub. • Configure Data Connector. • Enable out-of-the-box threat analytics rules using default values. • Deploy Workbook: ○ Threat Intelligence	1	ANS	Phase 2: Delivery	Phase1: Prerequisites	See 0
Configure Unified SecOps via Defender XDR Portal: • Connect Sentinel Workspace to Defender XDR. • Verify connection.	1	ANS	Phase 2: Delivery	Phase1: Prerequisites	
Deploy Additional Workbooks (from template only): • Workspace Usage • Sentinel Cost • Security Operations Efficiency • Data Collection Health Monitoring	1	ANS	Phase 2: Delivery	Phase1: Prerequisites	
Handover of Sentinel to [CUSTOMER] Workshop	1	ANS	Phase 3: Handover	Phase2: Delivery	

2.2.3 End of Workshop

Delivery - Microsoft Sentinel					
Deliverable	**Qty**	**Delivered by**	**Phase**	**Dependencies**	**Comments**
Customer Questionnaire	1	Customer	Phase 4: End of Workshop	Phase 3: Handover	This is required to be completed to

One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676

Delivery - Microsoft Sentinel					
Deliverable	**Qty**	**Delivered by**	**Phase**	**Dependencies**	**Comments**
					qualify the funding available.
Presentation & Next Steps Discussion	1	ANS (Pre-Sales/Sales)	Phase 4: End of Workshop	Phase 3: Handover	AM/AE to arrange Meeting
[CUSTOMER] to complete post engagement questionnaire	1	Customer	Phase 4: End of Workshop	Phase 3: Handover	
Decommission Sentinel and Licences	1	Customer	Phase 4: End of Workshop	Phase 3: Handover	Customer will be liable for all costs and management of Sentinel if left in place after the Workshop period.

2.3 Accounts & Permissions

This section contains all the initial user accounts and permissions we require to implement Sentinel into [CUSTOMER]s environment.

There is 1 group of permissions ANS will need for the deployment of Sentinel.

2.3.1 Local Security Reader (optional)

[CUSTOMER] has requested a security review of the current security baseline as part of the MDR service, a local account with security reader will be required to enable ANS to undertake the review.

2.3.2 Local Administrator (Implementation)

Our Cloud Consultants will require local administration accounts to be setup in order to implement and configure the initial Sentinel service, once completed any accounts will need to be removed by [CUSTOMER].

2.3.3 Accounts and Permissions

2.3.3.1 Sentinel Implementation

The permissions listed below are what is required to onboard a customer to the ANS MDR service if Sentinel is not implemented, however this is subject to change and is dependent on the outcomes of the Statement of works, the roles below assume ANS will need to carry out all implementation tasks in [CUSTOMER] environment.

The roles in this document are **Mandatory and** are required for ANS to implement Sentinel.

ANS Role	Task	Type	Roles Type	Roles	Active /Eligible	Require Approval	Duration	Why ANS needs these permissions
Foundational Configuration. The permissions in this phase will be subject to the outcomes of the discovery phase, ANS will advise [CUSTOMER] which roles are required.								
Security Architects	Sentinel Implementation-Configuration	Local	Entra ID	Security Reader	Active	No	Onboarding Only	The Security engineers assigned to implement Sentinel and/or configure Sentinel will require security reader in order to review the baseline architect and recommend changes

One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676

ANS Role	Task	Type	Roles Type	Roles	Active /Eligible	Require Approval	Duration	Why ANS needs these permissions
								to the MDR service if required.
Security Engineer	Sentinel Implementation Configuration	Local	Entra ID	Security Reader	Active	No	Onboarding Only	
	Sentinel Implementation Configuration	Local	Entra ID	Security Admin	Eligible	Recommend Yes	Onboarding Only	
	Sentinel Implementation Configuration	Local	RBAC	Owner on subscription to assign Service Principal permissions (Reduce to Contributor on resource group once work is completed) *	Active	Yes	Onboarding Only	
	Sentinel Implementation Service Principal	Local	Entra ID	Hybrid Identity Administrator	Eligible	Recommend Yes	Onboarding Only	
Other considerations **[CUSTOMER] cannot grant one or more roles.** In the circumstances that internal governance policies are preventing [CUSTOMER] from granting one or more roles, [CUSTOMER] should contact the ANS AM and or Presales as soon as possible to discuss alternatives such as template deployments with your own engineers. *Alternatively use contributor and assign responsibility of allocating SP roles to the customer.								

2.3.4 Post implementation review.

ANS will review the setup and seek sign off from the customer that the Sentinel deployment has been built and tested in accordance with this SOW. At this stage ANS/[CUSTOMER] will remove/disable any accounts and permissions no longer required.

2.4 Deployment Model

This section covers the high-level deployment model and method that will be used to deploy/configure Sentinel.

Existing Sentinel Implementation	Answer
Launch Deployment Required	Yes
Deployment Type	New
Deployment Model	Single
Azure Tenant ID	Here
Naming convention	Standard Microsoft

2.5 Deployment Design

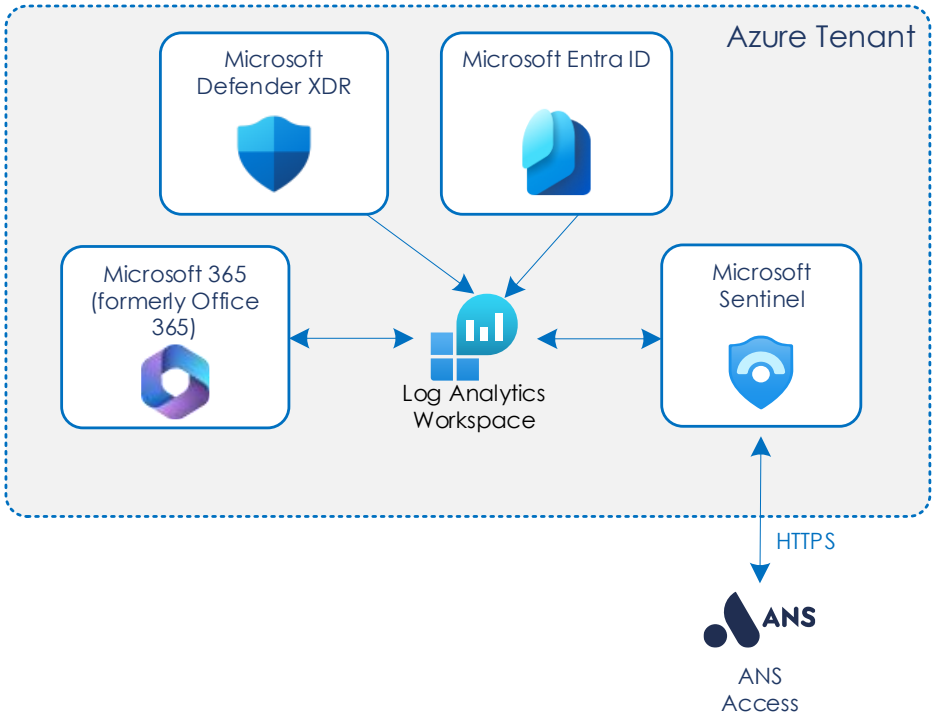
2.5.1 Single Deployment

For Sentinel Workshop deployment only 1 deployment model for Sentinel is used. This model also supports a co-managed approach to Sentinel where our customers may want to onboard to the ANS MDR service at a later date.

One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676



One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676

3. Sentinel Design

3.1 Sentinel Architecture

This section contains all the variables that ANS requires to be able to deploy Sentinel either through automation or through a manual installation. ANS will endeavour to use automation where possible to ensure a rapid deployment. In the case that Sentinel is already deployed then we still require this information for reference.

Variable type	Variable
Requires ALZ	No
Azure Subscription	Existing | To be created
Current Subscription name	Existing | To be created
Current Subscription name ID	Existing | To be created
Azure Licence model	Enterprise Agreements (EA) | Cloud Solution Provider (CSP)
Location	UK West UK South
Azure Resource Group	Existing | To be created
Current Resource Group name	Existing | To be created
Log Analytics Workspace	Existing | To be created
Log Analytics Workspace Name	Existing | To be created
Daily Cap Required (GB)	Proof of Concept – not required
Default days Retention	Default 90 Days
Sentinel Pricing Tier	Pay as you go | Commitment tier

Please Note – if an existing workspace is used [CUSTOMER] will not qualify for free data ingestion during this engagement. Only a workspace created in a Modern SecOps Engagement sponsored subscription will assure that costs are not billed.

3.2 Sentinel Content Hub Solutions

As part of the workshop engagement the following solutions need to be deployed via the Sentinel Content Hub:

Content Hub Solution	Data Connector	Analytics Rules / Playbooks	Enable Rules / Playbooks	Workbooks
Microsoft Defender XDR	Microsoft Defender XDR	Deploy all	5 x High Rules	None
Entra ID	Entra ID When enabling only Sign-in and Audit logs will be selected.	Deploy all	5 x High Rules	Microsoft Entra ID Sign-in logs Microsoft Entra ID Audit Logs
Microsoft 365	Microsoft 365 When enabling only Exchange, SharePoint and Teams will be selected.	Deploy all	5 x High Rules	Office 365 Exchange Online SharePoint & OneDrive
Azure Activity	Azure Activity	Deploy all	5 x High Rules	Azure Activity
Microsoft Defender Threat Intelligence	Microsoft Defender Threat Intelligence ALL available will be selected.	Deploy all	-	Threat Intelligence

3.2.1 Additional Workbooks

All additional workbooks will be installed from existing workbooks templates the additional workbooks to be deployed as part of this workshop are:

- Workspace Usage.
- Sentinel Cost.
- Sentinel Cost Optimisation.
- Security Operations Efficiency.
- Data Collection Health Monitoring.

One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676

4. Partner Admin Link (PAL)

To enable ANS to deliver the work described within this Statement of Work and provide the SLA's noted in any applicable Service Description for co-managed services, we require [CUSTOMER] Azure tenancy has ANS' ID set as the PAL prior to any deployment work taking place.

Microsoft partners provide services that help customers achieve business and mission objectives using Microsoft products. When acting on behalf of the customer, managing, configuring, and supporting Azure services, partner users will need access to [CUSTOMER]'s environment. Using Partner Admin Link (PAL), partners can associate their partner network ID with the credentials used for service delivery.

PAL enables Microsoft to identify and recognise partners who drive Azure customer success. Microsoft can attribute influence and Azure consumed revenue to your organisation based on the account's permissions (Azure role) and scope (subscription, resource group, resource).

ANS will require [CUSTOMER] to provide ANS with 'Contributor' access to all subscriptions we will need to be deploying resources into as part of the work described in this Statement of Work.

ANS will then run the following Azure CLI commands:

- **Connect-AzAccount -TenantId XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX**
  - XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX – Being [CUSTOMER]'s Azure Tenant ID which will be derived from the initial technical workshops.
- **new-AzManagementPartner -PartnerId 1070684**

ANS requires this PAL to be in-place for the lifecycle of the resources being deployed with the Azure tenancy.

Partner Admin Link (PAL) enables Microsoft to identify and recognise those partners who are helping customers achieve business objectives and realise value in the cloud. Customers must first provide a partner access to their Azure resource. Once access is granted, the partners Microsoft Partner Network ID (MPN ID) is associated. This association helps Microsoft understand the ecosystem of IT service providers and to refine the tools and programs needed to best support our common customers.

The PAL association to existing credentials provides no new customer data to Microsoft. It simply provides the telemetry to Microsoft where a partner is actively involved in a customer's Azure environment. Microsoft can attribute influence and Azure consumed revenue from the customer environment to the partner organisation based on the account permissions (Azure role) and scope (Management Group, Subscription, Resource group, Resource) provided by the partner to the customer.

PAL association only adds partner's MPN ID to the credential already provisioned and it does not alter any permissions (Azure role) or provide additional Azure service to the partner or Microsoft.

5. Assumptions & Exclusions

This Statement of Work is based on a Fixed Price basis, ANS herein are based on a defined amount to complete the tasks involved, regardless of project overrun or underrun.

- All work is to be carried out during normal working hours, Monday to Friday, 9.00am to 5.30pm unless otherwise stated.
- The quotation and any subsequent order are based on this Statement of Works. ANS Group will be pleased to cost any alterations and amendments and submit a new Statement of Works.
- All prerequisites[see] will be completed before the commencement of this project, and any deviation from this will be reported to ANS.
- All licences have [see] been procured before the commencement of this project, and any deviation from this will be reported to ANS.
- All permissions as stated in section 2.3 have been preapproved by [CUSTOMER].
- The consumption estimated provided by ANS is purely an estimate and is not commitment due to the large number of variables outside ANS scope of control.
- Anything outside the scope of this SoW will not be covered.
- [CUSTOMER] will be responsible for the Microsoft Sentinel and Log Analytics workspace consumption costs. Please note free consumption (provided free by Microsoft not ANS) of 10GB per day is only available for the first 30 days of the Workshop.
- Working with third parties not scoped as part of this Statement of Work (SOW) is not in scope.
- Any custom deployment not identified in this Statement of Work (SOW) is not in scope.
- Deployment is limited to the data connectors detailed in Section 0.
- [CUSTOMER] will make appropriate staff available to consultants working on this SOW.
- Changes will be made by [CUSTOMER] within 2 business days (unless otherwise agreed with the ANS Project Manager).
- [CUSTOMER] Information requested by ANS to be provided within 2 business days (unless otherwise agreed with the ANS Project Manager).
- This SOW only covers a single Sentinel instance.
- If [CUSTOMER] wish to subsequently onboard to the ANS MDR service, a separate Statement of Work will be produced to cover the onboarding to the MDR service.

ANS
One Archway
Birley Fields
Manchester, M15 5QJ
0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk
Co. Reg No. 3176761
VAT No. 245684676

6. Appendix

6.1 [CUSTOMER] Scoping sheet

Insert original scoping sheet tables.

One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676

7. Marketing Agreement

As part of this project [CUSTOMER] agree to the following Promotional and Marketing obligations in conjunction with ANS Group and Microsoft:

- Win announcement quote with [CUSTOMER] or similar comment to commence before project starts.
- Permission to use logo on ANS website and LinkedIn for Win Announcement

7.1 Optional on agreement

- Access to [CUSTOMER] contact to present the solution at a suitable event.
- Written Case Study on completion of project detailing final solution detailing initial challenges, how the work was carried out and what benefits have been gained.
- Video Case Study on completion.
- Use of the case study for promotional material and seminars.

All the above activities will be written by ANS Group marketing and signed off by Client named contacts below. Nothing will be released without confirmation from all contacts.

Approval List			
Name	**Role**	**Telephone**	**E-mail**

One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676

Accepted on behalf of [CUSTOMER]

By signing this Contract you confirm you accept the Supplier Terms and Conditions located at **http://www.ans.co.uk/site-info/terms-conditions**

Project Title: **[CUSTOMER] –** Modern SecOps Envisioning Workshop **- Statement of Work**

Project Status & Version: v.1

Name: {{_es_:signer2:fullname}} **Signed**: {{_es_:signer2:signature}}

Purchase Order Number: {{*PONUMBER_es_:signer2}} Date: {{_es_:signer2:date }}

Pre-Sales Confirmation Signature	
Signature	{{_es_:signer1:signature}}
Name	{{_es_:signer1:fullname}}
Date	{{_es_:signer1:date }}

One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676