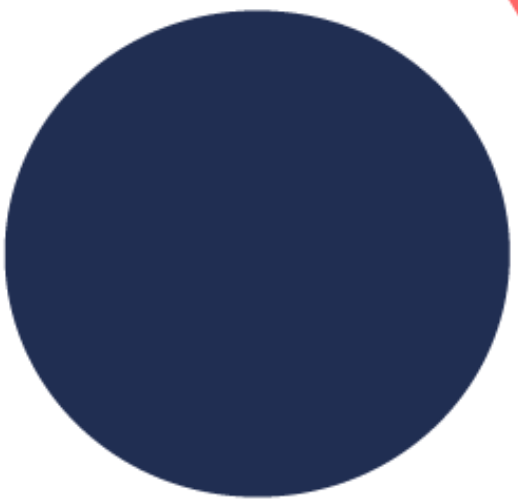
Microsoft Threat Protection Workshop

Statement of Work

For [CUSTOMER]



Contents

Notice

ISO Document Control

Document Control	
Document Name	Microsoft Threat Protection Workshop Statement of Work for [CUSTOMER]
Date Originated	27/01/25
Status	V0.4
Document Author	
Document Owner	
Approved by	
SOW Valid Until	4 weeks from issue date

Version Control	
Version Stage	New Document
Document Creation	27/01/25
First Draft V1.0	27/01/25

Document Team			
Name	**Role**	**Telephone**	**E-mail**

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

1. Purpose

The purpose of this document is to outline the key deliverables required to design and implement Microsoft Sentinel and M365 Security services within the [CUSTOMER]s tenant as part of a Microsoft Threat Protection 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 delivery 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 and M365 Security Proof of Concept.

ANS understands that [CUSTOMER] is looking to bolster their wider security posture and have identified Sentinel and M365 Security as tools for protecting from, detecting, investigating, and responding to cyber threats. ANS will deliver a fully functioning Microsoft Sentinel and Defender platform ready for data to be ingested and interpreted.

1.1. [CUSTOMER] Overview

AM/AE to complete – info about customer, what they do and why they want/need an MDR service.

Detail things like:

- Little bit of background on what they do.
- Customers need for this Workshop.
- Future security operations and tooling aspirations and plans.

1.2. [CUSTOMER] Contact Details

The contact details below will be the initial contact point for ANS during the deployment of the Threat Protection Workshop.

Name	Role	Email	Telephone
Customer	Details	Here	And here
Customer	Details	Here	And here

1.3. Engagement Type

This document is the statement of work to deliver the Threat Protection Workshop (typically a Microsoft funded engagement), at a high level it includes.

- Implementation of a single Sentinel instance in [CUSTOMER] tenant.
- Implementation of M365 Security tools and configuration.
- Demonstration of Security Copilot capabilities.

1.4. Document Scope

This document will cover the following:

- High level deliverables.
- Delivery process.

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

Issue No: 0.4 Issue Date: 27/01/25

- Prerequisites.
- Deployment model.
- Azure Lighthouse.
- Permissions.
- HLD design of the Sentinel configuration including
    - Subscription.
    - Resource group.
    - Log Analytic Workspace.
    - Microsoft Sentinel:
        - Pricing Tier.
        - Data retention.
        - Data connectors.
        - RBAC roles.

1.5. Deployment Scope

[CUSTOMER] require a new Sentinel Deployment and Microsoft Security Tooling, and the deployment scope includes:

- Configuration of the following mandatory modules and each of the included products:
    - Microsoft Defender Portal
        - Microsoft Defender XDR
    - Cloud Identity Protection
        - Microsoft Entra ID Protection
        - Microsoft Entra Conditional Access, unless Security Defaults has been enabled on the tenant, with three (3) conditional access rules created based on following conditional access templates:
            - Require multifactor authentication for risky sign-ins
            - Require password change for high-risk users
            - Block legacy authentication
            - Require multifactor authentication for admins
- Completion of at least three (3) of the following selectable modules:
    - Unified SecOps Platform
        - The following Data Connectors must be enabled:
            - Microsoft Defender XDR
        - Option 1 – Server Log Ingestion: A minimum of two (2) Windows servers forwarding logs to Azure Monitor (for use by Microsoft Sentinel).
        - Option 2 – 3rd Party Log Ingestion: Configure any 3rd party log ingestion data source using Content Hub Solution.
    - Email Protection
        - Microsoft Defender for Office 365 Evaluation mode
        - Microsoft Defender for Office 365 Attack Simulation
            - Attack Simulation training was delivered to at least ten (10) users.
    - Endpoint and Cloud Apps Protection

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

- Cloud app discovery
  - Cloud app usage logs must be collected using either alternative:
    - Microsoft Defender for Cloud Apps, using cloud discovery log one-time upload.
    - Microsoft Defender for Endpoint as a source of the cloud discovery logs, integrated with Microsoft Defender for Cloud Apps.
- Microsoft Defender for Endpoint
  - A separate device group must be created for the engagement, containing a minimum of five (5) Windows 10/11 devices enabled for Microsoft Defender for Endpoint.
    NOTE: these can be customer's devices onboarded to the Microsoft Defender for Endpoint during this engagement, or devices which the customer had onboarded to Microsoft Defender for Endpoint prior to the engagement.
- Microsoft Defender Vulnerability Management
  - A minimum of five (5) Windows 10/11 devices added to the Microsoft Defender Vulnerability Management security baseline assessment.

- Server Protection
  - Microsoft Defender for Cloud
    - Defender CSPM
      - Defender for CSPM must be enabled on at least one (1) subscription with Agentless Scanning for machines enabled for a minimum of five (5) Windows or Linux servers.
    - Defender for Servers
      - Defender for Servers Plan 1 must be enabled for a minimum of five (5) Windows or Linux servers.
- Identity Protection
  - Microsoft Defender for Identity
    - A minimum of three (3) domain controllers onboarded Microsoft Defender for Identity.
- Microsoft Security Copilot Demonstration
  - Deliver all the following Microsoft Security Copilot interactive experiences:
    - Unified SecOps Platform business email compromise
    - Defender XDR embedded to standalone Copilot
    - USOC - HumOR attack & Copilot embedded/standalone
    - Copilot - CISO report to the Board of Directors
    - Copilot - CISO using Security Copilot
    - Copilot for Security - Prompt book creation
    - Copilot - Script analysis

One Archway
Birley Fields
Manchester, M15 5QJ

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

Co. Reg No. 3176761
VAT No. 245684676

*If customer already has either security defaults enabled or has the rules or equivalent rules in place then this section can be skipped. However, ANS may require screenshots of the Conditional Access page or security defaults page.

1.6. Not in scope

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

- Configuration of Microsoft Security products beyond the guidance provided in this document.
- Deep analysis (investigation) of threats found during the engagement.
- Forensic analysis.
- Technical designs or implementations.
- Configuring non-Microsoft SIEM integration.
- Proof of Concept or Lab Deployment.
- Any ANS SOC Managed Services. This is only available if the ANS MDR service is being procured.
- 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, [CUSTOMER] can choose to implement this themselves.
- Additional Microsoft Sentinel Hunts, [CUSTOMER] can choose to implement this themselves.
- Additional configuration of M365 security services other than what is in scope to carry out the workshop.
- Any ITSM integration.
- Any Threat Intelligence integration.
- 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 Threat Protection Workshop.

2.1.1. Presales (This will be Completed prior to the SOW being issued)

- Scoping.
- Prerequisites.

2.1.2. Phase 1: Prerequisites

- Pre-Delivery Workshop (PDW).
- Review Prerequisites and confirmation completion.
- Schedule and confirm delivery milestones.
- Partner Admin Link (PAL).

2.1.3. Phase 2: Delivery – ANS

Note: If you are applying for funding all deliverables below must be completed to be eligible for funding, if [CUSTOMER] choose not to complete 1 or more of the deliverables below then ANS will charge the [CUSTOMER] a minimum of £8,000 for completion of the work.

- Configuration of the following mandatory modules and each of the included products:
    - Microsoft Defender Portal
        - Microsoft Defender XDR
    - Cloud Identity Protection
        - Microsoft Entra ID Protection
        - Microsoft Entra Conditional Access, unless Security Defaults has been enabled on the tenant, with three (3) conditional access rules created based on following conditional access templates:
            - Require multifactor authentication for risky sign-ins
            - Require password change for high-risk users
            - Block legacy authentication
            - Require multifactor authentication for admins
- Completion of at least three (3) of the following selectable modules:
    - Unified SecOps Platform
        - The following Data Connectors must be enabled:
            - Microsoft Defender XDR
        - Option 1 – Server Log Ingestion: A minimum of two (2) Windows servers forwarding logs to Azure Monitor (for use by Microsoft Sentinel).
        - Option 2 – 3rd Party Log Ingestion: Configure any 3rd party log ingestion data source using Content Hub Solution.
    - Email Protection
        - Microsoft Defender for Office 365 Evaluation mode
        - Microsoft Defender for Office 365 Attack Simulation
            - Attack Simulation training delivered to at least ten (10) users.
    - Endpoint and Cloud Apps Protection
        - Cloud app discovery

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

- Cloud app usage logs must be collected using either alternative:
  - Microsoft Defender for Cloud Apps, using cloud discovery log one-time upload.
  - Microsoft Defender for Endpoint as a source of the cloud discovery logs, integrated with Microsoft Defender for Cloud Apps.
- Microsoft Defender for Endpoint
  - A separate device group must be created for the engagement, containing a minimum of five (5) Windows 10/11 devices enabled for Microsoft Defender for Endpoint.
    NOTE: these can be customer's devices onboarded to the Microsoft Defender for Endpoint during this engagement, or devices which the customer had onboarded to Microsoft Defender for Endpoint prior to the engagement.
- Microsoft Defender Vulnerability Management
  - A minimum of five (5) Windows 10/11 devices added to the Microsoft Defender Vulnerability Management security baseline assessment.

- Server Protection
  - Microsoft Defender for Cloud
    - Defender CSPM
      - Defender for CSPM must be enabled on at least one (1) subscription with Agentless Scanning for machines enabled for a minimum of five (5) Windows or Linux servers.
    - Defender for Servers
      - Defender for Servers Plan 1 must be enabled for a minimum of five (5) Windows or Linux servers.
- Identity Protection
  - Microsoft Defender for Identity
    - A minimum of three (3) domain controllers onboarded to Microsoft Defender for Identity.
- Microsoft Security Copilot Demonstration
  - Deliver all the following Microsoft Security Copilot interactive experiences:
    - Unified SecOps Platform business email compromise
    - Defender XDR embedded to standalone Copilot
    - USOC - HumOR attack & Copilot embedded/standalone
    - Copilot - CISO report to the Board of Directors
    - Copilot - CISO using Security Copilot
    - Copilot for Security - Prompt book creation
    - Copilot - Script analysis

2.1.4. Phase 3: Handover | Decommission

- ANS and [CUSTOMER] Threat Protection Workshop Handover.

2.1.5. Phase 4: End of Workshop

- After 1 month of Sentinel ingesting logs the Microsoft Sentinel Workshop will be completed.

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 and [CUSTOMER] Proof of Execution (PoE), and Next Steps Discussion with ANS Account Manage/Executive and Pre-Sales.

2.2. Deliverables, Customer Requirements 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. Foundation delivery will generally be through an automated delivery process. For brand new implementations of Sentinel most of the work will be carried out by automation.

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. Customer Requirements

Successful delivery of the engagement is dependent on the [CUSTOMER] involvement in all aspects of the engagement. The customer must ensure that accurate and complete information is provided in a timely fashion as needed, that appropriate resources are committed, and that any activities are completed in a timely and effective manner.

The customer will need to perform the tasks, provide the resources, and take ownership of the following activities:

- The customer will need to provide adequate access to the necessary personnel needed to successfully complete the engagement, including:
    - A customer project manager responsible for the overall coordination and for scheduling logistics.
    - IT object owners for identity and security during all phases of the assessment.
    - An Executive Sponsor.
- The customer will provide the following to the delivery resource:
    - Access to any relevant documentation.

Executive Sponsor

- Owns the business case.
- Keeps project aligned with organization's strategy and portfolio direction.
- Governs project risk.
- Focuses on realization of benefits.
- Provides assurance.
- Suggested candidates: CSO, CISO, CEO, CFO, CIO or CTO.

We recommend making sure the executive sponsor participates in the following activities:

- **Error! Reference source not found.** or **Error! Reference source not found.**
- **Error! Reference source not found.**

Architects

- IT
- Security
- Network

One Archway
Birley Fields
Manchester, M15 5QJ

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

Co. Reg No. 3176761
VAT No. 245684676

- Server Infrastructure
- Identity

We recommend making sure the Architects participate in the following activities:

- **Error! Reference source not found.** or **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**

Administrators

- Security
- Network
- Server Infrastructure
- Identity
- Microsoft 365 and Azure Tenant Administrators

Security Architect

- Strong cybersecurity background and knowledge.
- Good understanding of Microsoft 365 and the security components of Microsoft 365.
- Good understanding of Azure and Azure Security Services.
- Has prior design experience with Microsoft security products, including:
    - Microsoft Entra ID
    - Microsoft Entra ID Protection
    - Microsoft Sentinel
    - Azure Log Analytics
    - Microsoft Defender XDR
    - Microsoft Defender for Office 365
    - Microsoft Defender for Cloud Apps
    - Microsoft Defender for Endpoint
    - Microsoft Defender Vulnerability Management
    - Microsoft Copilot for Security

Security Consultant

- Strong cybersecurity background and knowledge.
- Good understanding of Microsoft 365 and the security components of Microsoft 365.
- Good understanding of Azure and Azure Security Services.
- Has hands-on deployment experience with Microsoft security products, including:
    - Microsoft Entra
    - Microsoft Entra ID Protection
    - Microsoft Sentinel
    - Azure Log Analytics
    - Microsoft Defender XDR

One Archway
Birley Fields
Manchester, M15 5QJ

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

Co. Reg No. 3176761
VAT No. 245684676

- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Has hands-on deployment experience with Microsoft Defender for Endpoint.
- Has hands-on deployment experience with Microsoft Defender Vulnerability Management.

We recommend making sure the Administrators participate in the following activities:

- **Error! Reference source not found.** or **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**.

Commented [DH1]: Replace with my version (table)

2.2.2. Prerequisites

Prerequisites - Accounts and Permissions					
Deliverable	**Qty**	**Delivered by**	**Phase**		**Comments**
Azure Tenant and Azure Landing Zone in Place	1	Customer	Phase1: Prerequisites	Complete Scope sheet	
Creation of a suitable security subscription or other subscription suitable for Sentinel	1	Customer	Phase1: Prerequisites	Complete Scope sheet	
Customer to review permissions required for both [CUSTOMER] and ANS	1	Customer	Phase1: Prerequisites		See 2.3
Customer to provide any PIM/Identity Governance requirements before implementation	1	Customer	Phase1: Prerequisites	Complete Scope sheet	To ensure conforms to customer identity governance.
Create Entra administration accounts for ANS Engineer	1	Customer	Phase1: Prerequisites	Complete Scope sheet	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	Complete Scope sheet	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	Complete Scope sheet	

One Archway
Birley Fields
Manchester, M15 5QJ

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

Co. Reg No. 3176761
VAT No. 245684676

Prerequisites - Licences					
Deploy Threat Protection Engagement Microsoft 365 trial licences.	1	Customer	Phase1: Prerequisites		It is recommended that this is done just prior to the Delivery phase.
Prerequisites - Partner Admin Link (PAL)					
Partner Admin Link (PAL) Setup	1	ANS & Customer	Phase1: Prerequisites	-	Please refer to Section 5 for more information about PAL.

2.2.3. Delivery

Delivery -General				
Deliverable	**Qty**	**Delivered by**	**Phase**	**Comments**
Kick off Call | Documentation	1	ANS and Customer	Phase 2: Delivery	
Complete Threat Protection – Design Decisions Points document.	1	ANS and Customer	Phase 2: Delivery	
Implement Trial licences				

Delivery - Entra ID Protection				
Deliverable	**Qty**	**Delivered by**	**Phase**	**Comments**
Entra ID Identity Protection Deployment and Configuration	1	ANS	Phase 2: Delivery	
Configure and deploy Conditional access rules. • Require multifactor authentication for risky sign-ins • Require password change for high-risk users • Block legacy authentication • Require multifactor authentication for admins	2	ANS	Phase 2: Delivery	If rules already exist or have equivalent rules take a screenshot and skip this step. If Security defaults are enabled skip this step.

Delivery – Defender XDR				
Deliverable	**Qty**	**Delivered by**	**Phase**	**Comments**
Enable Defender XDR portal	1	ANS and Customer	Phase 2: Delivery	
Microsoft Defender for Endpoint Deployment (Customer) and Configuration (ANS) 5 x Windows 10/11 Endpoints will need to be deployed to.	1	ANS and Customer	Phase 2: Delivery	Customer will need to select and deploy to Endpoints – ANS will provide Guidance
Microsoft Defender for Endpoint Vulnerability management Deployment (Customer) and Configuration (ANS) 5 x Windows 10/11 Endpoints will need to be deployed to.	1	ANS and Customer	Phase 2: Delivery	

Delivery – Defender for Cloud Apps				
Deliverable	**Qty**	**Delivered by**	**Phase**	**Comments**
Microsoft Defender for Cloud Apps Deployment and Configuration (Discovery mode only)	1	ANS	Phase 2: Delivery	
Microsoft Defender for Cloud Apps, import of Firewall logs | or use Defender for Endpoint	1	Customer	Phase 2: Delivery	

Delivery – Defender for M365				
Deliverable	**Qty**	**Delivered by**	**Phase**	**Comments**
M365 Defender Deployment and Configuration.	1	ANS	Phase 2: Delivery	
Microsoft Defender for Office 365 Deployment and Configuration Deploy in audit mode.	1	ANS	Phase 2: Delivery	
Microsoft Defender for Office 365 Deployment and Configuration Prepare [1] Attack Simulator using out of the box templates.	1	ANS	Phase 2: Delivery	

Delivery – Defender for M365				
Deliverable	**Qty**	**Delivered by**	**Phase**	**Comments**
Microsoft Defender for Office 365 Deployment and Configuration Run [1] Attack Simulator using out of the box templates.	1	ANS	Phase 2: Delivery	

Delivery - Microsoft Sentinel				
Deliverable	**Qty**	**Delivered by**	**Phase**	**Comments**
Design of Microsoft Sentinel in [CUSTOMER] tenant and production of an HLD	1	ANS	Phase 2: Delivery	ANS will produce a low-level design for the Sentinel implementation.
Creation of security subscription	1	Customer | ANS	Phase 2: Delivery	Recommended but optional to create a separate security subscription.
Creation of log analytics workspace	1	ANS	Phase 2: Delivery	This will be deployed via automation.
Implementation of Microsoft Sentinel in X Azure Region	1	ANS	Phase 2: Delivery	This will be deployed via automation.
Configuration of workshop connectors • Microsoft Defender XDR • Windows Security Event via AMA	1	ANS	Phase 2: Delivery	See 4.2
Configuration of workshop connectors • Microsoft Defender XDR • Windows Security Event via AMA	1	ANS	Phase 2: Delivery	See 4.3
Implement the AMA agent on 2 servers, either on premises using Azure ARC or in Azure	2	Customer	Phase 2: Delivery	ANS will provide up to [2] hours consultation for deploying Azure ARC.
Enable up to 5 analytic rules per connector	10	Customer	Phase 2: Delivery	
Instruct [CUSTOMER] how to enable other rules				Optional
Connect Sentinel Workspace to Defender XDR Unified SecOps	1	ANS	Phase 3; Handover	
Handover of Sentinel to [CUSTOMER] Workshop	1	ANS	Phase 3: Handover	

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 Copilot for Security Demonstration				
Deliverable	**Qty**	**Delivered by**	**Phase**	**Comments**
Cover the following Copilot for Security Demonstration via Screenshare with Aventum: ○ Unified SecOps Platform – Business Email Compromise ○ Unified SecOps Platform – SAP Attack Disruption ○ Defender XDR embedded to standalone ○ USOC - HumOR attack & Copilot embedded/standalone ○ Copilot - CISO report to the Board of Directors ○ Copilot - CISO using Copilot for Security ○ Copilot for Security - Prompt book creation • Copilot for Security - Script analysis	1	ANS – Security Pre-Sales	Phase 2: Delivery	

2.2.4. End of Workshop

Delivery - Microsoft Sentinel					
Deliverable	**Qty**	**Delivered by**	**Phase**	**Dependencies**	**Comments**
Produce Proof of Execution (PoE)	1	ANS	Phase 4: End of Workshop	Phase 3: Handover	PoE to be supplied to Microsoft.
Next Steps Discussion	1	ANS (Pre-Sales/Sales)	Phase 4: End of Workshop	Phase 3: Handover	AM/AE to arrange Meeting
Decommission Sentinel and or Defender XDR tooling	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.

One Archway
Birley Fields
Manchester, M15 5QJ

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

Co. Reg No. 3176761
VAT No. 245684676

2.3.2. Local Administrator (Implementation)

Our SOC engineers will require local administration accounts to be setup in order to implement and configure the initial Sentinel service, once completed any accounts not required will be removed.

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**, [CUSTOMER] require 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	Azure AD	Security Reader	Active	No	Deployment 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 to the MDR service if required.
Security Engineer	Sentinel Implementation Configuration	Local	Azure AD	Security Reader	Active	No	Deployment Only	
	Sentinel Implementation Configuration	Local	Azure AD	Security Admin	Eligible	Recommend Yes	Deployment Only	
	Sentinel Implementation Configuration	Local	RBAC	Owner on subscription to assign Service Principal permissions (Reduce to Contributor on resource group once SP work and GitHub work is completed) *	Active	Yes	Deployment Only	
	Sentinel Implementation Service Principal	Local	Azure AD	Hybrid Identity Administrator	Eligible	Recommend Yes	Deployment 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 M365 Security Tooling has been deployed and the foundational Sentinel service has been built and tested. At this stage ANS 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.

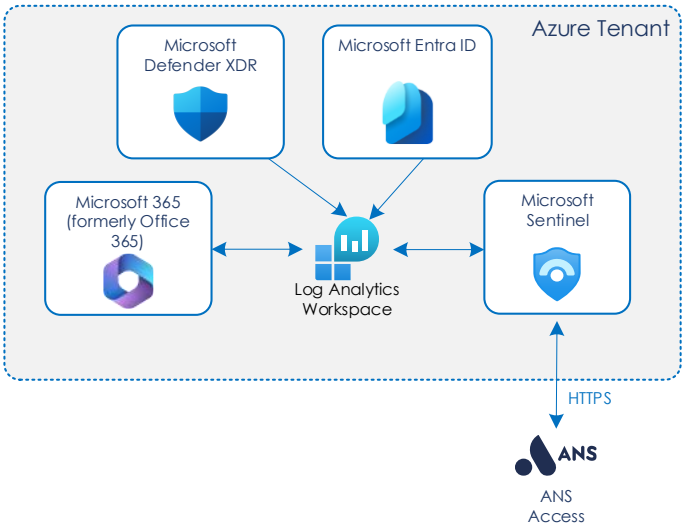
M365 Security Implementation	Answer
Launch Deployment Required	Yes
Deployment Type	New
Deployment Model for M365 Security Tooling	Single Tenant
Azure Tenant ID	Here
Products to Deploy	Microsoft Defender XDR Defender for Endpoint Plan 2 Defender for Office 365 Defender for Cloud Apps Defender Vulnerability Management
Number of Endpoints ANS to provide Deployment Assistance with	5

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 Threat Protection Workshop deployment only 1 deployment model for Sentinel is used, this is usually down to the customer only having one tenant and only operation in one region. This model also supports a co-managed approach to Sentinel where our customers may want to onboard to the ANS MDR services 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

3. Microsoft Defender XDR Security Tooling Design

Microsoft Defender XDR Security Tooling design will be completed as part of this engagement and recorded in the Threat Protection – Design Decision Points document.

4. Sentinel Design

Microsoft Sentinel design will be completed as part of this engagement and recorded in the Threat Protection – Design Decision Points document, this section is included for information only.

4.1. 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.

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

* If an Azure Landing Zone (ALZ) is required to be deployed this SOW cannot be progressed until one is in place. The customer can engage with ANS to have an ALZ deployed, please speak to your AM/AE.

4.2. Sentinel Connectors

The following connectors will be configured and implemented by ANS.

- **Service:** What service/sources requires connection to Sentinel.
- **Connector:** The equivalent connector available from Microsoft.
- **Licenced:** What licence is required and if [CUSTOMER] is licenced.
- **Status:** If the connector is already deployed or requires deployment.
- **Library connector:** Is the connector requested is already in the Microsoft or ANS library or requires bespoke development.

- **Health Check:** If the connector has been preinstalled by a non-ANS engineer, ANS will check the connector.
- **Deployed by:** Auto means the connector will be deployed automatically; Manual means the connector will be manually installed by an ANS engineer.
- **Log Analytics table:** This is the log analytics table the connector will write to.
- **Default Log Type**: This will be the default data pricing tier the connector will be implemented with please refer to SD document.
- **Interactive Retention:** Number of days the connector data configured for interactive data.
- **Archive:** Number of days the connector data configured for archiving.
- **Foundational/Advanced connectors:** Foundational connectors are implemented on the onboarding phase and typically deployed with automation, advanced connectors are installed in the transition period and often have dependencies like a log forwarder.

Service/Connector	To Deploy	Licenced	Mandatory	Notes	Interactive Retention	Archive
Windows Server via AMA	Yes	Yes	Yes	-	90	0
Microsoft Defender XDR	Yes	Yes	Yes	-	90	0

4.3. Sentinel Analytics Rules

Sentinel Analytics rules from the Content Hub for the following Content will be deployed as part of the Workshop:

- Microsoft Entra ID - Content Hub Analytics Rules only.
- Microsoft Defender XDR - Content Hub Analytics Rules only.

4.4. Sentinel Hunts

One Sentinel Hunt will be deployed as part of the Workshop. A minimum of 1 and a maximum of 3 Hunting Queries (included with Microsoft Sentinel Content Hub) will be deployed with the Hunt.

4.5. Sentinel Workbooks

No Sentinel Workbooks will be deployed as part of this workshop.

4.6. Sentinel Automation

No Sentinel Automation will be deployed as part of this workshop.

5. 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.

6. 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 4.2.
- [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.

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**

Accepted on behalf of <COMPANY NAME>

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:.....

Project Status & Version:.....

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

Purchase Order Number: {{*PONUM ner2}} Date: {{_es_:signer2:date }}

<**TITLE & VERSION** MUST BE ADDED FOR AUDIT

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