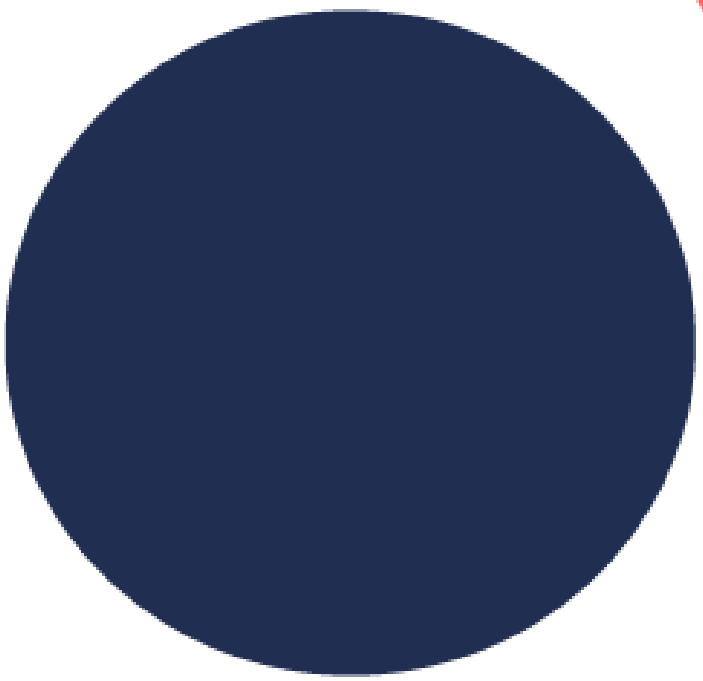
ANS Cybersecurity Assessment

Statement of Work



Contents

ISO Document Control **4**
Document Control 4
Version Control 4
Document Team 4
Document Distribution 4
1. Purpose **5**
1.1 Assessment Objectives 5
1.2 Overview 5
1.3 Contact details 5
1.4 Engagement Type 6
1.5 Document Scope 6
1.6 Assessment - In Scope 6
1.7 Assessment - Not in scope 6
1.8 Document validity 7
2. Assessment Overview **8**
2.1 Assessment Process 8
2.2 Prerequisites 8
2.2.1.1 General M365 8
2.2.1.2 Accounts and Permissions 9
2.2.1.3 Device Groups 9
3. Assessment Engagement **10**
3.1 Stage 1 - Pre-Engagement Call 10
3.1.1 Objective 10
3.2 Stage 2 - Cybersecurity Questionnaire 10
3.2.1 Objective 10
3.3 Stage 3 – Engagement Setup 10
3.3.1 Objective 11
3.4 Stage 4 – Change Management (Optional) 11
3.4.1 Objective 11
3.5 Stage 5 – Configuration 11
3.5.1 Stage 5.1 - General Configuration 11
3.5.1.1 Objective 11
3.5.2 Stage 5.2 - Microsoft Defender Vulnerability Management Configuration 12

One Archway
Birley Fields
Manchester, M15 5QJ

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

Co. Reg No. 3176761
VAT No. 245684676

3.5.2.1 Objective 12
3.5.3 Stage 5.3 – Insider Risk Management Analytics Configuration 12
3.5.3.1 Objective 12
3.5.4 Stage 5.4 - Cloud Discovery Log Collection (Optional) 12
3.6 Stage 6 – Exploration 13
3.6.1 Stage 6.1 – Vulnerabilities Exploration 13
3.6.1.1 Objective 13
3.6.2 Stage 6.2 – Data Security Exploration 13
3.6.2.1 Objective 13
3.6.3 Stage 6.3 – Cloud Discovery Exploration (Optional) 13
3.6.3.1 Objective 14
3.7 Stage 7 – Results Presentation 14
3.8 Engagement Decommissioning 14
3.8.1 Objective 14
4. Proof of Execution (PoE) – If funding applied 15
4.1 Microsoft 365 Defender - Settings 15
4.2 Microsoft 365 Defender – Devices 16
4.3 Microsoft Defender Vulnerability Management Device Discovery 16
4.4 Insider Risk Analytics – Scan Results 17
4.5 PoE Validation 17
5. Assumptions & Exclusions 18

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	ANS Cybersecurity Assessment Statement of Work
Date Originated	06/02/2024
Status	v0.1
Document Author	XXXX
Document Owner	XXXXX
Approved by	XXXX
SOW Valid Until	4 weeks from issue date

Version Control	
Version Stage	New Document
Document Creation	06/02/2024
V1.0 Issue Date	06/02/2024

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

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 activities and deliverables as part of the ANS Cybersecurity Assessment.

This Cybersecurity Assessment is delivered free of charge on the assumption that has been approved for funding by Microsoft and ANS are allowed to share proof of delivery to Microsoft to qualify the funding following delivery.

OR

The Cybersecurity Assessment is delivered as an initial stage of a wider Managed Detection and Response (MDR) contract, to better understand your Cybersecurity Maturity and ensure that an acceptable baseline for both you and ANS is achieved before onboarding the MDR service to the ANS SOC.

ANS understands that you are looking to better understand their Cybersecurity maturity, and where possible improve this with actionable recommendations.

1.1 Assessment Objectives

The objectives of this Cybersecurity Assessment are:

- **Understand current cybersecurity maturity level:** Help you understand their current cybersecurity maturity level using a questionnaire based on the CIS Critical Security Controls v8, providing recommendations and guidance on the next steps to improve your cybersecurity posture.
- **Discover and understand how to address vulnerabilities on clients and servers:** Help you understand how to use Microsoft Defender Vulnerability Management to discover, prioritise and address vulnerabilities and misconfigurations across clients and servers within the organisation.
- **Discover and analyse cloud application usage (Optional):** Help you understand your current cloud application usage using Microsoft Defender for Cloud, demonstrating how to detect and block risky applications.
- **Discover and understand risk related to data security and insider threats:** Help you understand the possible sensitive information that exists in their Microsoft 365 environment and the types of actions users are performing on that data that could be seen as potentially risky activities.
- **Define next steps:** The customer will work together with the delivery resource to define a list of next steps based on their needs, objectives, and results from the Cybersecurity Assessment.

1.2 Overview

ANS will work with you to understand what you do and why you want/need run this Cybersecurity service.

1.3 Contact details

The contact details below will be the initial contact point for ANS during the Cybersecurity Assessment.

Name	Role	Email	Telephone

One Archway
Birley Fields
Manchester, M15 5QJ

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

Co. Reg No. 3176761
VAT No. 245684676

1.4 Engagement Type

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

- Implementation of Microsoft Sentinel in your tenant.

1.5 Document Scope

This document will cover the following:

- High Level Assessment Overview.
- Prerequisites.
- Engagement Setup.
- Data Collection.
- Exploration.
- Results Presentation.
- End of Assessment and Decommissioning.

1.6 Assessment - In Scope

ANS will carry out a Cybersecurity Assessment with you, with the assessment scope including:

- Analysis of the ANS Cybersecurity Assessment Questionnaire once completed and returned by you.
- Deployment of Cybersecurity Assessment Microsoft 365 trial licences in your tenant (if required).
- Configuration of the Microsoft Product used as part of this assessment.
- Remediation of potential technical issues during the deployment (where reasonable).
- Scanning and assessment of vulnerabilities on on-premises Windows servers and clients within a single Active Directory domain.
- Exploration of vulnerabilities to discover and prioritise vulnerabilities and misconfigurations.
- Exploration of the sensitive information identified in the Microsoft 365 environment using out-of-the-box Microsoft Purview capabilities.
- Optional analysis of cloud applications used by users in your environment through Cloud Discovery as part of Microsoft Defender for Cloud Apps, based on either Defender for Endpoint or a one-time manual upload of logs from a single on-premises perimeter security device such as a firewall or proxy server.
- Decommissioning of configuration and licences at the end of the engagement.

1.7 Assessment - Not in scope

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

- Configuration of Microsoft or other tooling not covered in this document.
- Scanning and assessment of vulnerabilities on machine outside of corporate on-premises networks.
- Automatic upload of firewall or proxy server logs to Microsoft Defender for Cloud Apps (through a log collector).
- Analysis (investigation) of security incidents.
- Forensic Analysis.
- Technical designs or implementations.

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

1.8 Document validity

Due to the ever-evolving nature of these assessments, this statement of works has a validity date shown below, If the Statement of Works is not reviewed and signed by you on this date, ANS will need to review the Statement of Works and may need to issue a new one. This is to ensure that your requirements align to the latest Cybersecurity Assessment criteria.

[date] (28 days from issue).

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. Assessment Overview

2.1 Assessment Process

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

- Presales Stage:
  - This SOW to be produced, reviewed, and signed by you.
- Stage 1 – Pre-Engagement Call
  - Provide an overview of the engagement and agree, scope, schedule and required resources.
- Stage 2 – Prepare and Send the Cybersecurtiy Questionnaire
  - ANS will prepare and send the Cybersecurity Questionnaire to you following the Pre-Engagement Call.
- Stage 3 – Engagement Setup
  - To finalise the scope and configuration of the engagement tools.
- Stage 4 – Change Management (Optional)
  - Obtain necessary approvals for the deployment of the engagement tools. This is only necessary of your change control processes need to be followed as part of this engagement.
- Stage 5 – Configuration
  - Deploy Cybersecurity Assessment Microsoft 365 trial licences (if required) and configuration of the relevant security products.
    - Stage 5.1 – General Configuration
    - Stage 5.2 - Defender Vulnerability Management Configuration.
    - Stage 5.3 - Insider Risk Management Analytics Configuration.
    - Stage 5.4 - Cloud Log Discovery Log Collection (Optional).
- Stage 6 – Exploration
  - Work with you to analyse and document:
    - Stage 6.1 - Vulnerabilities Exploration.
    - Stage 6.2 - Data Security Exploration.
    - Stage 6.3 - Cloud Discovery Exploration (Optional).
- Stage 7 – Results Presentation
  - ANS will present and discuss the threat results of the Cybersecurity Assessment with you and agree next steps.
- Stage 8 – Engagement Decommissioning

2.2 Prerequisites

This section contains details on the Prerequisites required to carry out this assessment successfully. The pre-requisites will be covered as part of Engagement Setup.

2.2.1.1 General M365

The following M365 facilities are required to complete this assessment:

- You must have an M365 Account.
- Trial licences must be deployed as part of this engagement (ANS will advise when to do this) unless licences have already been procured by you.
  - Clients - Microsoft Defender Vulnerability Management Add-on.
  - Servers - Microsoft Defender Vulnerability Management included as part of Defender for Servers Plan 2.

One Archway
Birley Fields
Manchester, M15 5QJ

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

Co. Reg No. 3176761
VAT No. 245684676

2.2.1.2 Accounts and Permissions

The following accounts and permissions are required for ANS to carry out the assessment:

- Customer to have users involved during the engagement with the following Entra ID roles:
  - Security Administrator role.
  - Security Reader role.
- Scanning Account – this must be a Group Managed Service Account (gMsa):
  - The account is a least privileged account with only the minimum required scanning permissions.
  - The account will be removed at the end of the engagement.
- Purview Account:
  - Membership in:
    - Insider Risk Management.
    - Information Protection.
    - Compliance Data Administrator (Microsoft Entra ID and Purview Roles).

Account setup will be covered during Engagement Setup.

2.2.1.3 Device Groups

A Device Group will be required to filter results from scanned devices. Device Groups will be covered during Engagement Setup.

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. Assessment Engagement

3.1 Stage 1 - Pre-Engagement Call

[CUSTOMER] Duration and Effort	Up to 1 Hour
[CUSTOMER] Resource Requirements	Security Operations M365 and Azure Tenant Administrators
Pre-Requisites	n/a

3.1.1 Objective

The objective of the Pre-Engagement Call is to provide an overview of the engagement and agree on the scope, schedule and required resources. The following items will be covered during the call:

- Introduce the ANS team to you and set the stage for the assessment.
- Introduce the Cybersecurity Assessment.
- Describe and discuss the upcoming activities.
- Align expectation and timelines.
- Allocate resources.
- Discuss Change Management process with you.
- Agree on a date for the questionnaire to be completed.

3.2 Stage 2 - Cybersecurity Questionnaire

[CUSTOMER] Duration and Effort	Approximately 1 Hour
[CUSTOMER] Resource Requirements	Security Operations
Pre-Requisites	Stage 1 – Pre-Engagement Call

3.2.1 Objective

The objectives for these activities are:

- ANS will prepare and send to you the Action Required email and Cybersecurity Assessment Questionnaire.
- You will need to complete and return the Cybersecurity Assessment Questionnaire to ANS.
- ANS will review the completed Cybersecurity Assessment Questionnaire once returned from the customer.

Please note - The completion of the questionnaire, including the analysis and resulting recommendations, is a critical component for a successful delivery of the Cybersecurity Assessment engagement. ANS will not be able to progress with the assessment until the completed questionnaire is returned.

3.3 Stage 3 – Engagement Setup

[CUSTOMER] Duration and Effort	Approximately 1 Hour
[CUSTOMER] Resource Requirements	M365 and Azure Tenant Administrators Security Operations
Pre-Requisites	Stage 2 – Cybersecurity Questionnaire

One Archway
Birley Fields
Manchester, M15 5QJ

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

Co. Reg No. 3176761
VAT No. 245684676

3.3.1 Objective

The objective is to finalise the scope and configuration of the engagement tools.

- ANS to provide an overview of the products involved in this accelerator:
  - Microsoft Defender Vulnerability Management.
  - Microsoft Purview Insider Risk Management.
- Discuss and decide on the engagement scope:
  - Microsoft Defender Vulnerability Management:
    - What devices (servers/clients) should be scanned for vulnerabilities.
  - Microsoft Defender for Cloud Apps:
    - How logs will be gathered.
  - Microsoft Purview Insider Risk Management.
- Design decisions and engagement scope will be recorded by ANS.

3.4 Stage 4 – Change Management (Optional)

[CUSTOMER] Duration and Effort	Dependent on your Change Control Process
[CUSTOMER] Resource Requirements	M365 and Azure Tenant Administrators Security Operations
Pre-Requisites	Stage 3 – Engagement Setup

3.4.1 Objective

The objectives for these activities are:

- Obtain necessary approvals for the deployment of the engagement tools as per agreed engagement scope.
- Change control approvals if required are the responsibility of you.

3.5 Stage 5 – Configuration

3.5.1 Stage 5.1 - General Configuration

[CUSTOMER] Duration and Effort	30 Minutes (Allow up to 1 Hour)
[CUSTOMER] Resource Requirements	M365 and Azure Tenant Administrators Security Operations
Pre-Requisites	Stage 3 – Engagement Setup Stage 4 – Change Management

3.5.1.1 Objective

The objective is to configure the included Microsoft 365 Defender security products included as part of the engagement in the customer tenant, particularly the following:

- Deploy Cybersecurity Assessment Microsoft 365 trial licenses required for the Microsoft 365 Defender security products and services used during the engagement in the customer tenant.
- Configure any required Microsoft 365 tenant settings.
- Configure Microsoft Defender for Cloud Apps (optional).

One Archway
Birley Fields
Manchester, M15 5QJ

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

Co. Reg No. 3176761
VAT No. 245684676

- Configure pre-requisites for Microsoft Defender Vulnerability Management Authenticated scan for Windows.

3.5.2 Stage 5.2 - Microsoft Defender Vulnerability Management Configuration

[CUSTOMER] Duration and Effort	1 Hour
[CUSTOMER] Resource Requirements	M365 and Azure Tenant Administrators Security Operations
Pre-Requisites	Stage 5.1 – General Configuration

3.5.2.1 Objective

The objective is to configure Microsoft Defender Vulnerability Management in the customer tenant, particularly the following:

- Configure Microsoft Defender for Endpoint, if required.
- Deploy the Microsoft Defender Vulnerability Management Authenticated scan for Windows scanner.
- Configuring a new Microsoft Defender Vulnerability Management Authenticated scan for Windows.

3.5.3 Stage 5.3 – Insider Risk Management Analytics Configuration

[CUSTOMER] Duration and Effort	30 Minutes (Allow up to 1 Hour)
[CUSTOMER] Resource Requirements	M365 and Azure Tenant Administrators Security Operations
Pre-Requisites	Stage 5.1 – General Configuration

3.5.3.1 Objective

The objective is to configure Microsoft Purview Insider Risk Management products included as part of the engagement in the customer tenant, particularly the following:

- Insider Risk Management Permissions.
- Insider Risk Management Analytics.

3.5.4 Stage 5.4 - Cloud Discovery Log Collection (Optional)

If it was decided to use logs from on-premises security devices like firewalls or proxy servers during the scoping activities in section 10.1 Engagement Setup and Scope Definition Meeting, use this activity to upload those logs to Microsoft Defender for Cloud Apps together with the customer.

NOTE: If it was decided to use Microsoft Defender for Endpoint as a source for the cloud discovery logs, then skip this activity.

[CUSTOMER] Duration and Effort	1 Hour
[CUSTOMER] Resource Requirements	M365 and Azure Tenant Administrators Security Operations Network Administrators
Pre-Requisites	Stage 5.1 – General Configuration

One Archway
Birley Fields
Manchester, M15 5QJ

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

Co. Reg No. 3176761
VAT No. 245684676

The objective is to create cloud discovery snapshot report(s) in Microsoft Defender for Cloud Apps by uploading log files from the customer's on-premises perimeter security device such as a firewall or proxy server that were collected and stored in FTP format during the Data Collection period.

3.6 Stage 6 – Exploration

3.6.1 Stage 6.1 – Vulnerabilities Exploration

[CUSTOMER] Duration and Effort	1 Hour
[CUSTOMER] Resource Requirements	M365 and Azure Tenant Administrators Security Operations
Pre-Requisites	Stage 5.1 – General Configuration Stage 5.2 – Microsoft Defender Vulnerability Management Configuration

3.6.1.1 Objective

The objective is for ANS and you to work together to analyse and document vulnerabilities and security recommendations as part of the Vulnerabilities Exploration activity, particularly the following:

- Exploration of vulnerabilities using Microsoft Defender Vulnerabilities Management.
- Exploration of recommended actions in Microsoft Secure Score.
- Optionally, explore the use of cloud applications discovered by Microsoft Defender for Cloud Apps.

3.6.2 Stage 6.2 – Data Security Exploration

[CUSTOMER] Duration and Effort	1 Hour
[CUSTOMER] Resource Requirements	M365 and Azure Tenant Administrators Security Operations
Pre-Requisites	Stage 5.1 – General Configuration Stage 5.4 – Insider Risk Management Analytics Configuration

3.6.2.1 Objective

The objective is for ANS and you to work together to analyse and document potential risks related to the storage and handling of sensitive data within the organization, particularly the following:

- Explore the types of sensitive information within the Microsoft 365 environment (SharePoint, Teams, OneDrive for Business, Exchange) through the use of trainable classifiers and sensitive info types in Microsoft Purview Information Protection
- Explore potential areas of risk identified in the handling of organizational data in Microsoft 365 through the use of Insider Risk Management Analytics.

3.6.3 Stage 6.3 – Cloud Discovery Exploration (Optional)

[CUSTOMER] Duration and Effort	1 Hour

One Archway
Birley Fields
Manchester, M15 5QJ

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

Co. Reg No. 3176761
VAT No. 245684676

[CUSTOMER] Resource Requirements	M365 and Azure Tenant Administrators Security Operations
Pre-Requisites	Stage 5.1 – General Configuration Stage 5.4 – Insider Risk Management Analytics Configuration

3.6.3.1 Objective

The objective is for ANS and you to work together to analyse and document the results of the Cloud Discovery Exploration, examining and recording the findings of cloud applications utilized by users within the customer's organization. Any connections to vulnerabilities or data security threats will be flagged.

3.7 Stage 7 – Results Presentation

[CUSTOMER] Duration and Effort	2 Hours
[CUSTOMER] Resource Requirements	Security Operations M365 and Azure Tenant Administrators Relevant Exec Sponsor
Pre-Requisites	Stage 6 - Exploration

- ANS to deliver the ANS Cybersecurity Assessment – Results and Next steps presentation to you.

3.8 Engagement Decommissioning

[CUSTOMER] Duration and Effort	1 Hour
[CUSTOMER] Resource Requirements	Security Operations M365 and Azure Tenant Administrators
Pre-Requisites	Stage 6 – Exploration Stage 7 – Results Presentation

3.8.1 Objective

The objective is to remove all the configuration and resources created in the customer tenant during the Cybersecurity Assessment.

- Decommissioning of Microsoft Purview Insider Risk Analytics.
- Decommissioning of Microsoft Defender Vulnerability Management and Microsoft Defender for Endpoint.
- Decommissioning of Microsoft 365 Defender Security Products.

One Archway
Birley Fields
Manchester, M15 5QJ

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

Co. Reg No. 3176761
VAT No. 245684676

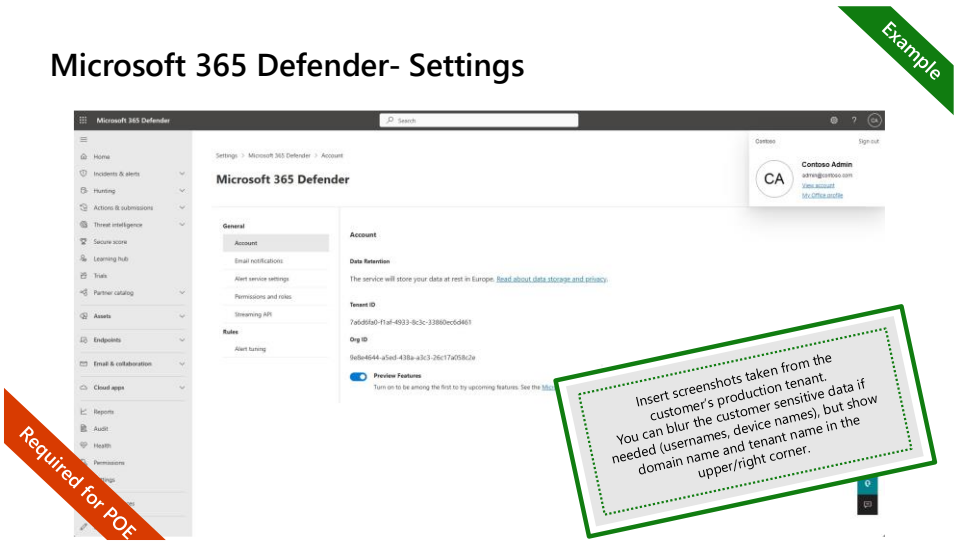
4. Proof of Execution (PoE) – If funding applied

To ensure successful delivery and approval of the Proof of Execution submission (in order to qualify for Microsoft Funding), the following deliverables are required:

- The completion of the questionnaire, including the analysis and resulting recommendations.
- Deployment and configuration of the following Microsoft products within your production tenant:
  - Microsoft Defender Vulnerability Management:
    - Scanning a minimum of 50 Windows 10/11 or Window Server machines.
  - Microsoft Purview Insider Risk Management Analytics.
- Prepare and discuss with the customer proposed next steps.

The following screenshots will be required from your tenant as part of the Proof of Execution:

4.1 Microsoft 365 Defender - Settings



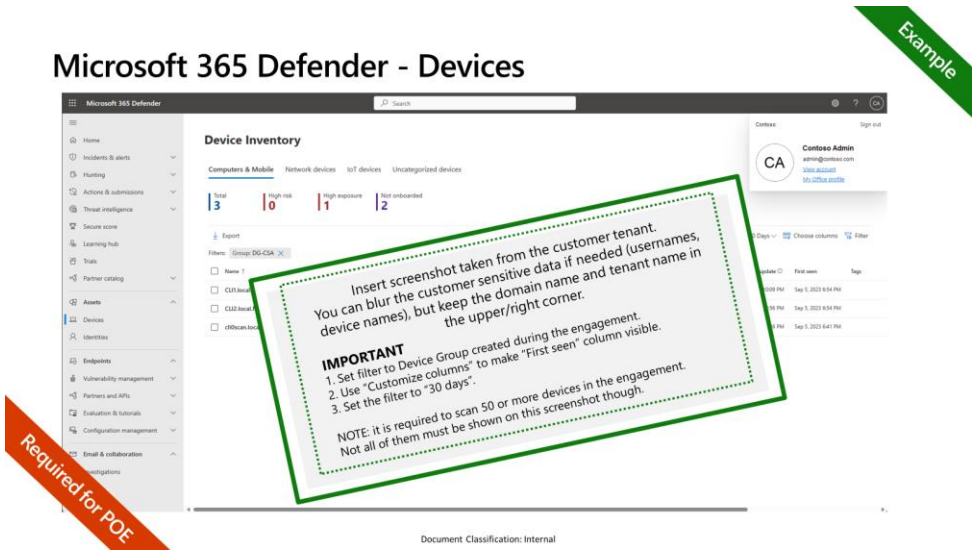
- Insert a screenshot from your production tenant – Settings > Microsoft 365 Defender > Account.
- Your sensitive information such as usernames and device names should be blurred.
- Must show domain name, tenant name in the upper/right corner.

One Archway
Birley Fields
Manchester, M15 5QJ

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

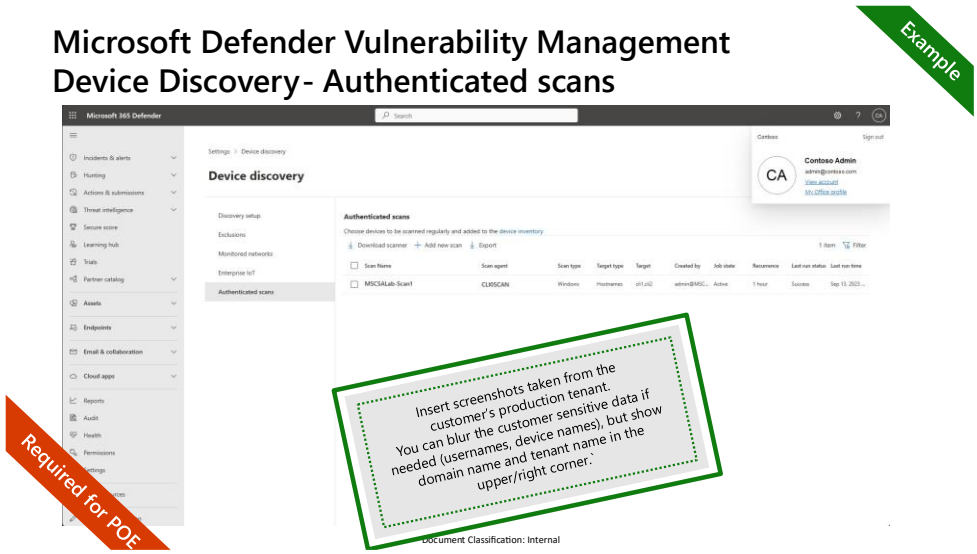
Co. Reg No. 3176761
VAT No. 245684676

4.2 Microsoft 365 Defender – Devices



- Insert a screenshot from your production tenant – Assets > Devices.
  - Set filter to Device Group created during this engagement.
  - Use "Customise columns" to make "first seen" column visible.
  - Set the filter to "30 days".
- Your sensitive information such as usernames and device names should be blurred.
- Must show domain name, tenant name in the upper/right corner.
- **Please Note** – it is required that 50 or more devices are scanned during this engagement, however not all of them must be shown on this screenshot.

4.3 Microsoft Defender Vulnerability Management Device Discovery

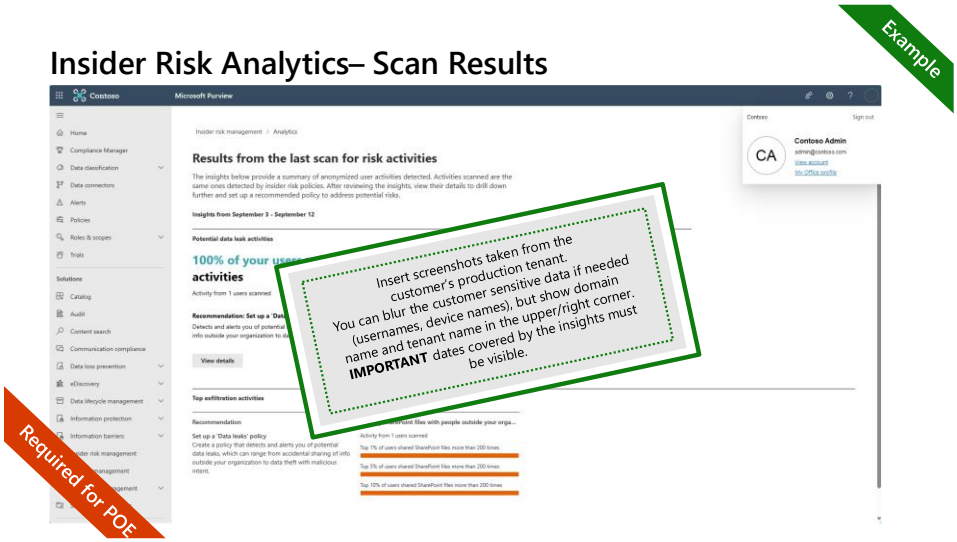


- Insert a screenshot from your production tenant – Settings > Device Discovery.
- Your sensitive information such as usernames and device names should be blurred.

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

- Must show domain name, tenant name in the upper/right corner.

4.4 Insider Risk Analytics – Scan Results



- Insert a screenshot from your production tenant – Purview > Insider risk management > Analytics.
- Your sensitive information such as usernames and device names should be blurred.
- Must show domain name, tenant name in the upper/right corner.

4.5 PoE Validation

ANS will send the PoE evidence to Microsoft to finally qualify for the funding. If for any reason the timescales and/or PoE evidence has not been achieved due to customer dependencies not being met, the customer may be liable to pay ANS for the Microsoft Sentinel 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

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.
- In the unlikely event of service downtime, the customer will arrange service downtime as required to complete the project.
- 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 [2.2.1.1] been procured before the commencement of this project, and any deviation from this will be reported to ANS.
- All permissions as stated in section[2.2.1.2] have been preapproved by you.
- Anything outside the scope of this SoW will not be covered.

One Archway
Birley Fields
Manchester, M15 5QJ

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

Co. Reg No. 3176761
VAT No. 245684676