Security Operations Navigator

Statement of Work and Scoping Document

Table of Contents

ISO Document Control

Document Control	
Document Name:	SecOps Navigator SOW and Scoping Document
Date Originated:	
Status	
Document Author:	
Document Owner:	
Approved by:	
Next Planned Review Date:	

Version Control	
Version Stage:	
Document Creation:	
V1.0 Issue Date:	

Document Team			
Name	Role	Phone	Email

Distribution List			
Name	Role	Phone	Email

1. Project Overview

The ANS SecOps Navigator is a consultative led exercise that involves a team of subject matter experts from ANS working with our customers to assess their business and technical requirements, review their current environments with a view to defining a clear strategic IT roadmap to implement at a pace to suit their needs. The Navigator process involves stakeholders from across the business and a team from ANS that work on multiple workstreams simultaneously.

The Navigator is designed to include a complete review of the existing security's technical and commercial environments with a view to setting the Target Architecture that will be implemented to address the business' technical and commercial goals and objectives. The ANS SecOps Navigator is designed using distinct workstreams that involves information gathering and processing at each stage. At the end of each stage of the Navigator, ANS will produce the relevant output related to that workstream and discuss this with the customer before moving on to the next stage. The aim of the SecOps Navigator is to work in partnership with your technical and operational teams to gain an accurate view of the existing network with a view to delivering a proposed architecture that meets the needs of your environment.

The outcome of the ANS SecOps Navigator will result in a business case and target architecture that can be implemented at pace and will align with the technical and commercial aspirations of your business.

2. Security Navigator

2.1. Overview

As part of the SecOps Navigator, the ANS Security Solutions Architect will perform series of workshops and assessments for you to gain an understanding of their current security landscape. We will review the existing security architecture and its capability to support a transition to cloud and digital in line with your business, technical & security strategy. ANS will work with you to understand their business objectives and to gain a clear understanding of your strategic IT roadmap, in particular how applications, services, end users, data and infrastructure will be secured, protected and compliant in the future.

2.2. Scope

This Navigator will cover the following areas:

1. Review of existing licencing.
2. Review of existing Cyber Security Governance and Strategy.

3. Review of existing Security Operations.
4. Review of security appliances and tooling.
5. Review of on-premises infrastructure.
6. Review of cloud infrastructure.
7. Review of Zero Trust policies.

2.3. SecOps Navigator Aim

The SecOps Navigator aim is to investigate your current security operations and provide advice on how to improve your Security Posture and Maturity.

2.4. ANS Approach

The SecOps Navigator is a free engagement between ANS and you and is not obliged to onboard any services from ANS after this engagement has ended, however ANS would appreciate that you complete the engagement and allows ANS to feed back their results. If at any point you wish to end the engagement early, please inform the account manage as soon as you can.

3. Customer Dependencies

There are several dependencies on you for the SecOps Navigator to be a successful engagement, primarily these are:

1. Completion of the scoping section (Section 5) of this document. Whilst some sections may be classed as business sensitive the SecOps Navigator is optimal if all questions are answered to the best of your ability.
2. Attendance of all the meetings, please advise the Account Manager if dates and times need to be changed.
3. All workshops are to be carried out during normal working hours, Monday to Friday, 9.00am to 5.30pm unless otherwise stated.
4. It is expected that the customer will provide all latest and up to date documentation including all commercials for infrastructure components such as hardware, software, and all associated licensing.
5. It is expected that [CUSTOMER] will provide a breakdown of all security personnel costs and roles.

4. Engagement process

The SecOps Navigator consists of 4 phases:

- Phase 1 - Meet and Greet
- Phase 2 - Workshop 1- Baseline Architecture
- Phase 3 - Workshop 2 - Proposed Target Architecture
- Phase 4 – Conclusion - where ANS will present back the findings in a PowerPoint presentation in which you can feed the results back to senior leadership or into a business case.

4.1. Phase 1 – Meet and Greet

4.1.1. Overview

The initial phase of the SecOps Navigator involves includes the Meet and Greet stage where the two project teams introduce themselves when ANS will clearly outline the SecOps Navigator process and milestones involved. The Meet and Greet can be held virtually on Teams or at a mutually agreed location for both project teams.

4.1.2. Prerequisites

- Attend the Meet and Greet with appropriate security personnel and stakeholders.
- Review the scoping questions in Section 5 and to ensure all questions can be answered and identify any questions/queries that need to be discussed with ANS during the Meet and Greet.
- Please contact the Account Manager/Sales Representative if you need to change the date and/or date of the Meet and Greet.

Phase 1	Length	Workshop Objectives
Meet and Greet	Maximum 60 mins	1. Meet and Greet. 2. Define Objectives. 3. Review Scoping Sheet.

4.2. Phase 2 – Workshop 1

4.2.1. Overview

In this workshop ANS will review their findings of the completed scoping sheet, run through the understanding of the baseline architecture, and discuss the initial proposals or possibilities of a target architecture that aligns with the business objectives. Finally, ANS will run through an initial Gap Analysis and high light the high-level tasks that the [customer] would need to complete to transform their baseline to target architectures with justifications for secure improvements and cost savings where possible.

4.2.2. Prerequisites

- Provide updated Scoping Question responses 5 working days prior to Workshop 1.
- Attend Workshop 1 with appropriate security personnel and stakeholders.
- Complete any actions from the Meet and Greet.
- Please contact the Account Manager/Sales Representative if you need to change the date and/or date of Workshop 1.

Phase 2	Length	Workshop Objectives
Workshop 1	Maximum 120 mins	1. Verify Scoping Sheet. 2. Review baseline architecture. 3. Discuss target architecture and justifications. 4. Agree scope of target architecture. 5. Discuss Gap analysis.

4.3. Phase 3 – Workshop 2

4.3.1. Overview

In this workshop ANS will propose their final proposed target architecture, a completed gap analysis, a prosed roadmap and outline the major work packages that would need to be completed by the [customer] to meet that proposed target architecture. Finally, ANS will identify any MSSP programs which you may be eligible for and outline any services from ANS that could help you meet that target architecture.

4.3.2. Prerequisites

- Complete any actions from Workshop 1.
- Attend Workshop 1 with appropriate security personnel and stakeholders.
- Please contact the Account Manager/Sales Representative if you need to change the date and/or date of Workshop 2.

Phase 3	Length	Objectives
Workshop 2	Maximum 120 mins	1. Review proposed target architecture. 2. Review gap analysis. 3. Review Proposed roadmap. 4. Review Proposed Work packages. 5. Discuss MSSP programs. 6. Discuss ANS services. 7. Agree final scope of output.

4.4. Phase 4 – Conclusion Meeting

In this phase ANS will go through the final output of the SecOps Navigator with you. There will be opportunity to ask questions and clarify any of the output during the meeting. ANS will take on board comments and where reasonable update the output presentation to reflect this. You will receive a copy of the presentation following the end of the meeting.

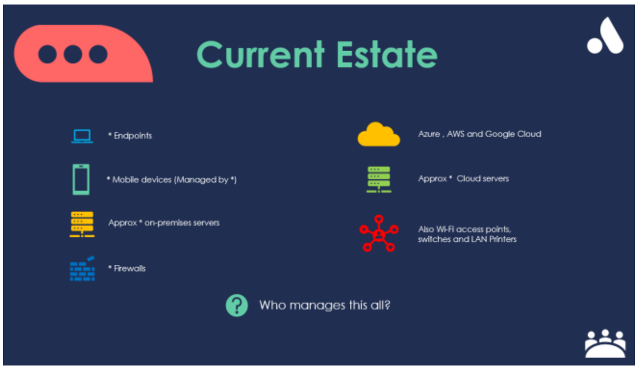
4.4.1. Prerequisites

- Complete any actions from Workshop 2.
- Attend the Conclusion Meeting with appropriate security personnel and stakeholders.
- Please contact the Account Manager/Sales Representative if you need to change the date and/or date of this meeting.

Phase	Length	Objectives
Workshop 2	Maximum 60 mins	1. Review Output. 2. Agree Content. 3. Agree any final changes (updated output to be provided directly – not an additional meeting).

4.5. Format

The output of the SecOps Navigator, this will be in the format of a PowerPoint presentation capturing all the output of the SecOps Navigator.



Current Estate

- * Endpoints
- * Mobile devices (Managed by *)
- Approx * on-premises servers
- * Firewalls
- Azure , AWS and Google Cloud
- Approx * Cloud servers
- Also Wi-Fi access points, switches and LAN Printers

Who manages this all?

5. Scoping Sheet

5.1. Instructions

Please complete the scoping questions to the best of your ability. If you have any queries or questions, please contact your Account Manager/Sales Representative.

Please answer all questions in the boxes highlighted in the colour below:

5.2. Customer Details

Customer Details	Answer
Company Name	
Company Website	
Contact(s)	
Email	
Company Bio	
Employees	
Customers	Please provide types of customers and if appropriate examples.
Countries Active in	

5.3. Microsoft Licences

Microsoft Licencing	Answer
Please list all Microsoft licences and quantities below:	
Office 365 Pro Plus:	
Office 365:	
Enterprise E1:	
Office 365:	
Enterprise E3:	
Office 365:	
Enterprise E5:	
Microsoft 365 Business:	Include what type of business account, basic, standard, or premium
Microsoft 365 E3:	
Microsoft 365 E5 suite features:	

Microsoft Licencing	Answer
Microsoft 365 Education A3:	
Microsoft 365 Education A5:	

Microsoft Usage	Answer
What, if any, Microsoft 365 services have you deployed?	
What, if any, Microsoft 365 security products have you deployed?	

5.4. Security and Governance Strategy

Security Strategy	Answer
So why now, what is driving the change?	
What are you trying to achieve?	
What are your priorities?	
Short Term - Priorities	
Mid Term - Priorities	
Long Term - Priorities	
Timelines - Ongoing? (If applicable)	
What is your Security Budget?	
What is your Modernisation Strategy?	
Technology Partner Strategy?	
Business Plan - ROI/TCO - Benefits - Considerations - Drivers	
Do you have a Zero Trust Strategy, if so, where are you on that strategy	

Security Concerns	Answer
Please list your security concerns	

Governance & Compliance	Answer
Do you have to meet any specific compliance obligations including laws, regulations, and standards? If so, which ones? Examples: HIPAA, GDPR, PCI DSS, etc.	
Are you aspiring to any compliance frameworks?	
Have you implemented a security control framework such as COBIT, ISO 27001 and/or NIST 800-53? If so, which one?	
Do you have Cyber Insurance, and if so with who?	
If no, is this something being considered?	
Do you have any timeframes we need to adhere to?	
What is your operational data retention?	
What is your security data retention?	

Security Audit	Answer
When was the last audit?	
How often do you hold them?	
Please provide details of a recent security audit if any (optional)?	
Do you carry out periodic Pen testing or ITHC?	
If so, how often?	
If so, please provide an overview of normal Critical and High findings.	

5.5. Security Operations

Current SOC Capability	Answer
Do you currently have a SOC/Security team?	
If this is managed by a 3rd party if so, who?	

Current SOC Capability	Answer
What SOC Roles (Analysts, CISO, architects, IS, SecDevOps) do you currently have?	
What is the SOC Size (people)?	
What is the SOC operational hours?	
What is the SOC SLA (Business hours)?	
What is the SOC SLA (Outside Business hours)?	
What is the SOC Setup (Tier 1, 2, 3)?	
Do you have SOC use cases?	
Qualifications (Please list all qualifications that the SOC team currently have.)	
Do you have custom use cases, if so, please provide an overview?	
MTTA: Mean time to acknowledge	
MTTR: Mean time to recovery	

Service Management	Answer
Do you have an IT Service Desk?	
What Service Desk Tool do you use?	
Managed internally/externally, if externally by who?	
Please provide an overview of your Incident Management Process.	
What are your DR processes - and SLA?	

Security Incidents	Answer
How many security incidents have you had in the last 12 months?	
What were the incidents in relation to?	
What remediation actions did you take?	

Major Incidents	Answer
In the event of a Major incident do you have:	
A Cybersecurity Response Plan	
A Disaster Recovery Plan.	
A Risk Management Plan (Identify, analyse, own , respond)	

User Education	Answer
What user education do you have regarding security?	
How often do staff have to refresh their training?	

5.6. Security Tooling

Security Tooling	Answer
Do you have any Layer 3 Firewalls?	
Do you have any Layer 7 Firewalls?	
Do you have a SIEM tool?	
Do have a SOAR tool?	
Do you use any XDR solutions?	
Do you use Site to Site or Client VPN solutions, please provide details?	
Do you have CASB facilities?	
Do you use an Identity Provider (AD,AAD, Hybrid)?	
Do you use any Vulnerability Management tools?	
Do you use any Asset Management tools?	
Do you use any Endpoint Manager tools?	
Do you use any Threat Intelligence facilities?	
What Anti-Virus / Endpoint Protection do you use?	
What Data Backup tooling do you use?	
Do you have any Information Protection tools?	
Do you have any Email Security tools/services?	
Have you secured emails with DMARC/DKIM/SPF and MTS-STS records	
Do you have any Web Security tools/services?	
Do you have any DNS Protection in place?	

Security Tooling	Answer
Do you have any DDOS Protection in place?	
Azure / Microsoft - Do you use security score, and do you review on a regular basis?	

5.7. Business Critical Applications

System	Hosted by	Managed by	RTO	RPO	Sensitive Data	Reason for Criticality (Such as revenue, emergency service etc.)	SLA
When purchasing cloud services do you adhere to the NCSC cloud security principles?	The cloud security principles - NCSC.GOV.UK						

5.8. Private Datacentre Infrastructure

On Prem Servers	Quantity	Operating System Version(s)	Endpoint Protection	Notes
Physical Servers:				
Windows				
Linux				
Virtual Servers:				
Windows				

Linux				

Networking / Peripherals	Quantity	Make	Model	Notes
Firewalls				
Switches				
Routers				
Wi-Fi Access Points				
Load Balancers				
LAN Printers				
Other 1				
Other 2				
Other 3				
Other 4				

Endpoints	Quantity	Operating System Version(s)	Endpoint Protection	Notes
Laptops/Desktops				
Windows				
Linux				
Mac				
Chromebook				

Mobile Devices	Quantity	MDM Used	Endpoint Protection	Notes
Managed Android				
Managed Apple				
BYOD Android				
BYOD Apple				

Networking	Type / Supplier	Number of Sites	Notes
Type of Internet Connection			
Type of Site-to-Site Connections (if applicable)			

Networking	Type / Supplier	Number of Sites	Notes
How do remote workers access your on Prem Systems?			

5.9. Public Cloud Infrastructure 1

Cloud Infrastructure	Answer	Notes
Vendor		
Tennant(s)		
Managed by		

Public Cloud Servers	Quantity	Operating System Version(s)	Endpoint Protection	Notes
Windows				
Linux				

Other Cloud Services	Quantity	What is it used for?	Notes
			e.g. Azure AD
			e.g. Databases
			e.g. Storage
			e.g. Defender for Cloud

5.10.Public Cloud Infrastructure 2 (Delete if not required)

Cloud Infrastructure	Answer	Notes
Vendor		
Tennant(s)		
Managed by		

Public Cloud Servers	Quantity	Operating System Version(s)	Endpoint Protection	Notes
Windows				
Linux				

Other Cloud Services	Quantity	What is it used for?	Notes
			e.g. Azure AD
			e.g. Databases
			e.g. Storage
			e.g. Defender for Cloud

5.11.Zero Trust Assessment

Identity		
Question	Answer	Notes
Have you enabled multifactor authentication for internal users?		All users/ some users/ admins only/ none
Which forms of password less authentication is enabled for your users?		Phone/text/oath token/Microsoft Auth App/Fido/Windows Hello
Which of your user groups are provisioned with single sign-on (SSO)?		
Which of the following security policy engines are you using to make access decisions for enterprise resources?		Cloud access security brokers (CASB) Security information and event management (SIEM) Endpoint Protection Mobile Device Management (MDM) Security Policy Engine Other
Have you disabled legacy authentication?		
Are you using real-time user and sign-in risk detections when evaluating access requests?		
Which of the following technologies have you integrated with your identity and access management solution?		Cloud access security brokers (CASB) Security information and event management (SIEM) Endpoint Protection Mobile Device Management (MDM)

Identity		
Question	Answer	Notes
		Security Policy Engine (for example, conditional access) Other
Which of the following context is used in your access policies?		User Application Type Network Location User risk Sign-in risk SIEM data Other
Have you implemented endpoint threat detection to enable real-time device risk evaluation?		all/some/not consistently
Do you use separate accounts for administration?		
Do you use PIM (Azure) Privileged Identity Management documentation - Microsoft Entra | Microsoft Learn		
Do you use access reviews in Azure? What are access reviews? - Azure Active Directory - Microsoft Entra | Microsoft Learn		

Endpoints		
Question	Answer	Notes
Are devices registered with your identity provider?		all/some/not consistently
Are devices enrolled in mobile device management for internal users?		all/some/not consistently
Are managed devices required to be compliant with IT configuration policies before granting access?		all/some/not consistently
Do you have a model for users to connect to organizational resources from unmanaged devices?		all/some/not consistently

Endpoints		
Question	Answer	Notes
Are devices enrolled in mobile device management for external users?		all/some/not consistently
Do you enforce data loss prevention policies on all managed and unmanaged devices?		all/some/not consistently

Data		
Question	Answer	Notes
Has your organization defined a data classification taxonomy?		all/some/not consistently
Are access decisions governed by data sensitivity rather than simple network perimeter controls?		all/some/not consistently
Is corporate data actively and continuously discovered by sensitivity in any location?		all/some/not consistently
Are data access decisions governed by policy and enforced by a cloud security policy engine? (e.g., available anywhere on internet)		all/some/not consistently
Are the most sensitive files persistently protected with encryption to prevent unauthorized access use?		all/some/not consistently
Are there data loss prevention controls in place to monitor, alert, or restrict the flow of sensitive information (for example, blocking email, uploads, or copying to USB)?		all/some/not consistently

infrastructure		
Question	Answer	Notes
Have you enabled cloud infrastructure protection solutions across your hybrid and multicloud digital estate?		all/some/not consistently

infrastructure		
Question	Answer	Notes
Does each workload have an app identity assigned?		all/some/not consistently
Are user and resource (machine-to-machine) access segmented for each workload?		all/some/not consistently
Does your security operations team have access to specialized threat detection tools for endpoints, email attacks, and identity attacks?		Yes/No/Limited
Does your security operations team have access to a security information and event management (SIEM) solution to aggregate and analyse events across multiple sources?		Yes/No/Limited
Does your security operations team use behaviour analytics to detect and investigate threats?		Yes/No/Limited
Does your security operations team use security orchestration, automation, and remediation (SOAR) tooling to reduce manual effort in threat response?		Yes/No/Limited
Do you regularly review administrative privileges (at least every 180 days) to ensure admins only have just enough administrative rights?		all/some/not consistently
Have you enabled Just-in-Time access for administration of servers and other infrastructure?		all/some/not consistently

Applications		
Question	Answer	Notes
Are you enforcing policy-based access controls for your applications?		all/some/not consistently

Are you enforcing policy-based session controls for your apps (for example, limit visibility or block download)?		all/some/not consistently
Have you connected business-critical apps to your app security platform to monitor cloud data and cloud threats?		all/some/not consistently
How many of your organization's private apps and resources are available without VPN or hardwired connection?		all/some/not consistently
Do you have ongoing Shadow IT Discovery, risk assessment, and control of unsanctioned apps?		all/some/not consistently
Is administrative access to applications provided Just-In-Time/Just-Enough-Privilege to reduce risk of permanent permissions?		all/some/not consistently

Network		
Question	Answer	Notes
Are your networks segmented to prevent lateral movement?		all/some/not consistently
What protections do you have in place to protect your networks? (Check all that apply)		External firewall Distributed denial-of-service (DDoS) attack protection Web application firewalls Other
Are you using secure access controls to protect your network?		all/some/not consistently
Do you encrypt all your network communication (including machine to machine) using certificates?		all/some/not consistently
re you using ML-based threat protection and filtering with context-based signals?		all/some/not consistently