Service Definition

ANS Protect XDR Plus

1. Operational Services

1.1. Terms and definitions

The definitions used in the Terms shall have the same meaning when used in this Service Definition. The following additional terms used in this Service Definition are defined as follows:

Term	Definition
Alert	the creation of a notification in relation to a Security Event that is not yet determined as malicious or harmful or a security Incident
ANS Glass	the portal where the Customer can log/view Service-related tickets, alerts and performance dashboards.
Artificial Intelligence	computer systems able to perform tasks normally requiring human intelligence.
Business Critical Incident	Incidents that cause complete outage or failure of systems or services identified by the Customer as crucial to normal business operations.
Change	the addition, modification, or removal of anything that could have a direct or indirect effect on the Service.
Containment	the process or implementation of a defined action as part of a strategy, during the handling of a Security Event that aims to minimize the scope of the Security Event and contain the effects of unauthorised activities within the environment.
Co-Managed	a partnership between the Customer and the Supplier to manage tooling, where the Supplier brings subject matter expertise to support effective operations.
Customer User	a User within the Customer organisation identified as entitled to receive the Service.
Detection	the platform capability to detect a threat or security Incident for which a response is required.
Digital Forensic Incident Response	to identify suspicious activity on the networks, determine who is creating the problem, contain the incident, and take steps to safeguard their infrastructure to prevent similar attacks in the future.

Emergency Change	a Change required in order to resolve or implement a tactical workaround for a P1 incident
Emergency Hours	17:31 to 08:59 Monday to Friday including bank holidays in England and 17:31 Friday to 08:59 Monday including bank holidays in England and all of Saturday and Sunday in England.
Endpoint	Endpoints are physical or virtual devices that create entry and exit points for data communication on a network. This definition refers to desktop computers, laptop computers and servers.
Eradication	the removal of suspicious or unauthorised resources in efforts to return the account to a known safe state. The eradication strategy depends on multiple factors, which depend on the business requirements for the Customer's organisation.
Fully-Managed	outsourcing the management and delivery of technical systems to the Supplier.
Incident Case	a software tool functionality that provides a structured and efficient approach to analyzing, investigating and responding to alerts generated by the customer security tooling.
Incident Response	the actions following the declaration of a Security Incident. This includes implementation of Containment measures where applicable, assessing risk and impact and Customer notification as per the Supplier's Security Incident Management process.
Item	a server, device, endpoint or application source for which a vulnerability or Security Event can be discovered.
Machine learning	Machine learning is an application of artificial intelligence that provides systems the ability to automatically learn and improve from experience without being explicitly programmed.
Major Security Incident	a significant Incident that has impact to multiple or critical IT systems that requires a combined, multi-team approach to resolve.

Malware	software or applications that seek to disrupt, damage, or gain unauthorized access to a computer system and compromise the organisation's operational functions.
Project Change	Change delivered by way of the Supplier's Professional Services.
Recovery	the action of this phase is to bring affected systems back into the production environment carefully, as to ensure that it will not lead another Incident.
Remediate	the actions to reverse, stop damage, improve or correct the actions affecting the IT environment.
Response	the action taken by the Supplier to acknowledge Alert/s and begin an investigation into the status of the Alert/s.
Security Event	any observable occurrence in a system or network that could indicate a potential security issue.
Security Incident	an unplanned Security Event that leads to an actual or potential breach of security policy or the security controls in place to protect data or systems.
Security Incident Management Process	A structured approach to identifying, managing, and resolving security incidents using recognised security frameworks as guidance (Identification, Containment, Eradication, Recovery, Lessons Learned).
Security Platform	Supplier's Security Platform that provides its own Security Orchestration, Automation and Response (SOAR) capabilities.
Service Desk	the primary point of contact between the Customer Users and Supplier for all Incidents and Service Requests.
Service Operation	the service is operated 24x7.
Service Request	a request from a Customer User for information, advice, or for access to a Service. A Service Request is also a request to execute a Standard Change.
SOC Analyst	an analyst working in the Security Operations Centre with security based technical skills who can analyse the data surrounding a Security Event.

Standard Change	a pre-authorized Change that is low risk and follows a documented process for implementation.
Table of Capabilities	the table contained in annex 1 to this Service Definition which articulates the scope of Services and details locations, platforms, devices and applications within scope for management by the Service.
Threat Hunting	is a proactive active cyber defence activity. It is the process of actively and iteratively searching through system data to detect and isolate advanced threats that have evade existing security solutions.
Threat Intelligence	Information of the intent and capabilities of malicious cyber threats, including the actors, tools, and TTPs, through the identification of trends, patterns, and emerging threats and risks, in order to inform technical detection tooling or to provide timely warnings;
TTPs	Tactics, Techniques, and Procedures being structured framework for understanding, analysing, and responding to cyberattacks by detailing the strategies, methods, and specific actions used by adversaries.
Vendor	the third-party software provider.
Vulnerability Intelligence	consolidation of data from multiple sources giving a contextualized assessment of organizational risk arising from identified vulnerabilities.
Vulnerability Scanning	assessment of the organisations assets in relation to known vulnerabilities.
Workload	Servers either databases, web applications, domain controllers, file servers etc.
Working Day	8.5 Normal Business Hours.
XDR	Extended Detection and Response (XDR) is a security solution that aims to identify, investigate, and respond to advanced threats that originate from various sources, including the cloud, networks, and email.
XDR plus	includes everything in the Supplier's EDR and XDR product tiers in terms of advanced threat intelligence with human expertise to provide threat detection, monitoring, and remediation.
24x7	24 hours a day, 7 days a week.

2. Overview

ANS Protect XDR Plus combines advanced threat intelligence with human expertise. Our Extended Detection and Response (XDR) Service provides prevention, detection and response capabilities. The additional Managed Service offers analysis and support from our qualified security experts, enhancing alert management and incident response.

2.1 A summary of the Service is as follows:

2.1.1 Management of supplied detection and response tooling;

2.1.2 Configuration of automated response features;

2.1.3 Automated Incident Response and Containment;

2.1.4 Endpoint monitoring, anomaly detection and threat intelligence;

2.1.5 Operational support via Glass portal;

2.1.6 SOC analyst response to XDR tooling alerts.

2.2 Service wrap:

2.2.1 Automated response and remediation through policy configuration and automation for response and remediation;

2.2.2 Policy creation and management;

2.2.3 Operational system management and support of associated platform and agents used by the technology to deliver the Service;

2.2.4 SOC analyst engagement to review and analyse XDR tooling alerts and provide incident response to malicious events.

3. Scope

3.1 The Supplier will;

3.1.1 Deploy and configure the technology;

3.1.2 configure relevant policy rules and security settings;

3.1.3 manage the Alert signals and proactively tune the system to reduce false positives;

3.1.4 conduct automated analysis and investigation of the Security Events generating the Alerts to determine the nature and status of the events;

3.1.5 provide automated Containment and eradication responses to the detected threats;

3.1.6 initiate automated Containment actions at the first indication of suspected or actual malicious behaviour;

3.1.7 use reasonable endeavours to deliver a Containment response in a timely manner;

3.1.8 configure and provide automated threat hunting, subject to being fully integrated with the Customer’s in scope technology;

3.1.9 fully manage the technical security solution provided to the Customer as described in the Table of Capabilities for XDR Plus;

3.1.10 provide engineering support to maintain the Service and deal with complex technical issues;

3.2 The Supplier will;

3.2.1 provide a secured Security Operations Centre (SOC) facility with operational resilience for business continuity;

3.2.2 provide trained SOC Analysts and other relevant staff to manage the scope of services and analyse alerts raised by the tooling;

3.2.3 provide a SOC facility with Supplier staff based in the United Kingdom;

3.2.4 provide security vetted staff that meet the security requirements of the Customer, at the Customer expense. Where Government level vetting is required, the Customer will sponsor all relevant Supplier staff;

3.2.5 provide managed threat detection and response that will be supported with automated rules and the use of Artificial Intelligence to assist in determining the nature and relevance of the threat. This also includes the automated process of deploying any appropriate Containment activity;

3.2.6 create a Security Incident and commence Incident Response procedures, where the Security Event is malicious;

3.3 provide Incident Response that will;

3.3.1 provide an Incident Response based off alerts generated by the existing automated technical tooling analysis and respond to suspicious Security Events detected within the defined scope of the Customer IT infrastructure;

3.3.2 provide a security response through appropriate Containment strategies applicable to the Security Event. The response will include remediation guidance to the Customer, operational support and resolver teams;

3.3.3 initiate Containment actions at the first indication of suspected or actual malicious behavior;

3.3.4 use reasonable endeavours to deliver a Containment response in a timely manner;

3.3.5 consider any automated response to an Alert or incident as a response in relation to the SLAs stated;

3.3.6 notify Customer named representatives via defined channels;

3.3.7 provide security notification 24/7 via defined channels;

3.3.8 managed incidents where a P1 Incident has been declared, this will be dropped to a P2 Incident once a successful Containment response has been applied;

3.3.9 **Incident Response and Escalation Table**

Priority	Response SLA	Specialist Review	Escalation Manager	Escalation Director/Vendor	Notification Frequency
P1	30 Minutes	1 Hour	Immediate	Immediate	Hourly Email
P2	1 Hour	2 Hours	4 Hours	6 Hours	GLASS Portal
P3	4 Hours	1 Day	2 Days	None	GLASS Portal

For an Incident, "Response" is the time from when the ticket is first logged within the ANS ITSM Tool to the time that the Supplier responds with a suitably qualified

Employed person whether via an email, GLASS Portal update, telephone call or in person.

From the time of Response until resolution, updates shall be provided to the contacts and/or escalation contacts named on the Customer account by email or ANS Glass portal updates at such frequencies as set out in the table above.

3.4 provide a Supplier operated Security Platform that will;

3.4.1 provide its own Security Orchestration, Automation and Response (SOAR) capabilities. The technology used will be at the Supplier's discretion ;

3.4.2 take identified data feeds from Customer tooling to enrich and manage through the Supplier defined processes;

3.4.3 apply additional Threat Intelligence augmentation to Alerts in the Security Platform for analysis in the platform;

3.4.4 correlate multiple alerts in the Security Platform into single Incident Case;

3.4.5 manage each individual Incident Case in the Security platform;

3.4.6 provide response playbooks/runbooks that are developed and used with in the Security Platform;

3.4.7 use at its discretion, automated processes in the Security Platform to accelerate the threat analysis, response and Containment to counter cyber threats in the Customer's scope of service;

3.4.8 provides Data segregation that is managed in the Security Platform. Only designated staff from the Supplier will have access and limited access will be provided to the Customer

3.4.9 provide Data residency in the United Kingdom for SOAR related tooling. Data is held in Google Data Centers (europe-west2) based around London, UK.

3.4.10 enable Data hosted in the Security platform to be encrypted using AES-256 encryption. Data in transit is protected with TLS 1.2 or higher.

3.4.11 enable Data security supported by DDoS protection and WAF services, monitoring of the data centre is undertaken by Google 24/7 and the platform logs are additionally monitored separately under the Supplier service provision. All data in the service is backed up by Google Secure Operations. A daily full backup snapshot is taken. Any Security incident involving Customer data in the Security Platform will be reported to the Customer;

3.4.12 provide a Security Platform that is configured to ensure high-availability;

3.5 provide a response level according to severity that will;

3.5.1 be provided through automated rules and the use of Artificial Intelligence to assist in determining the nature and relevance of the threat. This also includes the automated process of deploying any appropriate containment activity;

3.5.2 consider any automated response to an alert or incident as a response in relation to the SLAs previously stated;

3.5.3 have all Alerts and Incidents reviewed by the SOC Analysts;

4. Hours of service

4.1 Normal Business Hours are 9am to 17:30pm Monday to Friday (excluding Public holidays in the UK);

4.1.1 Service is available 24 hours a day, 365 days per year.

5. Service Levels, KPIs and Service Credits

Category	Service Level Target	Minimum Service Level	Service Credits
P1 Incidents	100% of Incidents will be responded to within 30 minutes.	100%	1st Incident missed response time will attract a 5% Service Credit. A 2nd Incident missed response time will attract a 10% Service Credit.
P2 Incidents	100% of Incidents responded to within 1 hour.	Service credits apply from 2nd failure within a calendar month	1st Incident missed response time will attract a 0% Service Credit. 2nd Incident missed response time will attract a 5% Service Credit. 3rd Incident missed response time will attract a 10% Service Credit;

Service Credits are calculated as a percentage of the monthly Base Charge and in any event, shall not exceed 10% of the monthly Base Charge in the month that the Service Credit arose.

Where a Service Credit is due, it shall not accumulate with any other Service Credit and only one Service Credit can be offered within the monthly period.

A miss on the agreed time is only applicable to the month that the miss occurred. Response times are recorded in the Suppliers ITSM tooling.

6. Customer Responsibilities

The Customer will:

6.1 provide the Supplier with technical access and relevant permissions to deliver the Service, including providing the Supplier with authorisation and technical access to enable automated response for Containment.

6.2 attend any Service orientation calls at the start of delivery of the Service, providing required information to support the successful implementation of the technical infrastructure;

6.3 assist the Supplier in the remediation of issues that may prevent operation of the Service;

6.4 advise the Supplier two (2) working days in advance of any penetration testing or additional vulnerability scanning so that the Supplier can apply the relevant context to the Alerts.

6.5 submit all Service Requests to the Service Desk, by telephone or electronically in ANS Glass by one of the designated named Customer's contacts;

6.6 attend meetings scheduled at mutually convenient times;

6.7 inform the Supplier, with a minimum of 5 working days' notice, of any Change that may impact the operation of the Service;

6.8 provide out of hours contact details for nominated individuals in order to be notified of any relevant Security Incident and provide Customer representation on Incidents;

6.9 update the Supplier of changes to nominated individuals on the Customer's account and associated contact details;

6.10 support the Supplier with timely decision making in order to enable the appropriate countermeasures to a Security Incident to be deployed or enacted;

6.11 will not hold the Supplier liable for any highly sophisticated or advanced threat actor attack that may occur that goes undetected by the tooling;

6.12 will not hold the Supplier liable for any impacts of a malicious attack by any third party retained by the Customer or malicious Customer insider;

6.13 apply all reasonable remediation recommendations to the in-scope environment. Where this is not implemented by the Customer within a reasonable time, the Supplier may increase the charges to accommodate for additional time and effort to detect and remediate recurring Security Events and Incidents. The Supplier's Standard Published Rates will apply;

6.14 acknowledge and respond to incidents escalated by the Supplier with individuals nominated by the Customer to be included in the Security Event notification process;

6.15 provide reasonable availability of Customer representative(s) when resolving a security related incident or request.

6.16 ensure that all Customer Supported Assets are appropriately licensed and have Supplier recommended hardware/software and vendor support in place.

6.17 Ensure that all packages are maintained and managed unless the Customer has subscribed to a package management service

6.18 Ensure on-going availability of suitable internet connection (if not provided by the Supplier);

6.19 report Business Critical Incidents via telephone only. The Supplier cannot offer the Service Levels or Service Credits for Business-Critical Incidents raised via email.

6.20 pre-authorise the Supplier to make changes to the Detection ruleset and policies without a Change Request or written Customer agreement. The Supplier will always act in good faith in implementing or tuning the rules to provide the best prevention, detection and response services to the Customer;

6.21 acknowledge any changes by the Customer that disrupt the Service will be subject to Additional Service Charges, at the Supplier's Standard Published Rates, to rectify and remediate;

6.22 The Supplier will not proceed without the Customer's authorisation where Additional Service Charges are to be raised. The Customer shall be liable for such Additional Service Charges and any consequential liability where the Customer does not authorise the Supplier to proceed with the additional work. allow and enable the Supplier to electronically map any AWS or Azure environment for the purpose of incident response and assessment. Output can be shared with the Customer;

7. Assumptions

7.1 All Customer Supported accounts covered by a valid software maintenance and support agreement in line with this Contract Service Levels.

7.2 All Customer Supported Assets are in a valid supported configuration at the Commencement Date.

7.3 All Customer specific pre-requisites have been completed at the Commencement Date.

7.4 The Customer will provide resources to work with the Supplier to on-board the Service, and assist with maintenance tasks as required.
The Service is agreed on the principle of an acceptable use limit. The Customer may be liable for Additional Service Charges based on any spikes in consumption due to Customer activities

7.5 Work done by the Supplier on the Customer's environment remains the intellectual property of the Supplier;

7.6 If the Customer requires the Supplier to provide onsite hands and eyes support, then this will be subject to Additional Service Charges.

7.7 provide Emergency Change guidance as required to remediate Security Incidents and in the event of a significant and/or destructive Security Incident, the Supplier may need to apply a short-term Containment action before formal Customer approval is received. The Supplier will act in good faith and the Customer will not hold the Supplier liable for any of these actions or variable outcomes;

8. Exclusions

The following are listed as exclusions to this service:

Note - This list shall not be considered complete or exhaustive and the applicable Terms should be consulted;

8.1 Issues resulting from misconfiguration by the Customer of the Customer Supported Assets and scope of service, resulting in impact to the Service;
8.2 Issues resulting from failures in maintenance/administration by the Customer of the scope of service resulting in impact to the Service;
8.3 Issues resulting from unauthorised access by the Customer of the scope of service;
8.4 Issues create by the Customer on systems that affect the scope of service that impact the ability for the Supplier to deliver the Service;
8.5 End User or 1st line support;
8.6 Technical advice to any persons not listed as a named contact on te Customer's account;
8.7 Failure to meet SLA due to public cloud provider outages;
8.8 Project Changes are excluded from the Service and will be subject to Additional Service Charges. Project Changes are recorded within ANS Glass for informational and approval purposes only;
8.9 Emergency Changes that are not a direct output of a Priority 1 incident may be subject to Additional Service Charges;
8.10 Existing compromises prior to being live in service with the Supplier will be treated as a chargeable project to remediate in order to be accepted into service;
8.11 The Customer's technology failing to respond to an execution command initiated by the Supplier to a Containment activity;
8.12 The Supplier does not provide vendor integrated Digital Forensic Response retainer Services;
8.13 The Supplier does not share any intellectual property created in support of the service with the Customer;
8.14 The service is not an IT Operational service monitoring or problem identification service and is not responsible for IT operational under performance issue identification;
8.15 The Supplier will not include Digital Forensic Analysis where Incident Management is provided. Advice and guidance will be provided on selection of specialist 3rd party expertise;
8.16 The Supplier will refer any actions or activities required that are outside of the contracted services to the customer with options for consideration and decision making. This may involve additional project work or professional services and Additional Service Charges;