Service Definition

SMB | Managed Detection and Response
inc. Carbon Black & Sentinel

Product Terms for MDR Package

The following Product Terms apply if the relevant Services are included within your Quotation. In the event of a conflict between the Product Terms and the applicable Terms and Conditions, these Product Terms shall prevail, but only to the extent of such conflict. Any capitalised terms used in this document shall have the meanings set out in the applicable Terms and Conditions (save where expressly provided otherwise below) and any additional definitions outlined below shall also apply.

1. Operational Services

1.1. Service Description

Normal Business Hours = 9:00 -17:30, Monday to Friday (excluding bank holidays)
Working Day – 8.5 Normal Business Hours
24x7 = 24 hours a day, 7 days a week

1.2. Service Overview

ANS Managed Detection and Response is an advanced threat hunting and incident response service to prevent, detect and respond to cyber threats in a single, easy-to-use solution. Customers are offered a choice of three tiers:

- **ANS Managed Detection and Response Base** offers the fundamentals of next generation antivirus (NGAV) to protect customers from modern cyber threats.
- **ANS Managed Detection and Response Pro** provides prevention, detection, and response capabilities to analyse and respond to cyber threats rapidly. It uses an automated threat response to ensure the environment is kept safe without needing any human resource to manage.
- **ANS Managed Detection and Response Business** combines advanced threat intelligence with human expertise to provide threat hunting, monitoring, and response. The ANS MDR Business is supported by our Security Operations Centre (SOC).

1.3. ANS Service

Service	Service Description	Service Hours	Base	Pro	Business
	Incident Management				
Priority Escalation to Vendor for faults	Priority escalation to Vendor Support for Platform & sensor/agent-based issues.	Normal Business Hours	✓	✓	✓

High Priority Escalation to Vendor	High Priority escalation to Vendor Support for Priority 1 business critical faults related to Platform & sensor/agent-based issues.	24 x 7	✓	✓	✓
Automated Malware Detection & Prevention	Automated prevention and removal of known malware, ransomware, and other malicious processes that may be running. Detection & Removal based off ANS produced threat intelligence feeds of known Indicators of Compromise (IoCs)	24 x 7	✓	✓	✓
False Positive Review	The Supplier will commit to review and remediation of false positives identified by the Customer occurring on Customer Supported Assets upon an Incident being submitted by the Customer to the Supplier.	Normal Business Hours	-	✓	✓
Security Incident Response	Provide data, interpretation, and remediation advice for Customer Incident response for P2, P3, P4 Security Incidents	Normal Business Hours	-	-	✓
High Priority Security Incident Response	Provide data, interpretation, and remediation advice for Customer Incident response for P1 Security Incidents	24 x 7	-	-	✓
Security Incident Remediation and Advice	Provide advice, response, and containment of P2, P3 or P4 Security Incident	Normal Business Hours	-	-	✓
High Priority Security Incident Remediation and Advice	Provide advice, response, and containment of P1 Security Incident	24 x 7	-	-	✓
Service Desk - Non-Business Critical Faults	The Supplier provides access with relevant ANS Portal or phone contact details to the Supplier Service Desk for non-critical system/service down and/or affected scenarios (P2/P3/P4) related to the ANS MDR platform.	Normal Business Hours	-	-	✓
Service Desk - Business Critical faults	The Supplier provides 24/7 access with relevant phone contact details to the Supplier Service Desk for critical system down scenarios (P1) only that are related to the ANS MDR platform.	24 x 7	-	-	✓

Change Management & Advisory					
Policy Maintenance	The Supplier will maintain the policy sets that apply to all client infrastructure. These policies define the protection levels of the service and outline inclusions and exclusions of files/folders to scan.	Normal Business Hours	✓	✓	✓
Automated Detection Rules Updating	The Supplier will configure and customise Malware Detection rules that will be updated with any new indicators of compromise & signatures when released.	24 x 7	✓	✓	✓
Policy Selection	The Supplier will support the changing of policy type per agent/sensor monitored. Policy types are built on the risk level of the device in question.	On Request	-	✓	✓
Device Isolation	The Supplier will configure Automated playbooks to isolate devices based on specific events as agreed with the Customer.	24 x 7	-	-	✓
Threat Hunting Detection	The Supplier will configure and customise threat hunting queries that will be updated and automatically run across all monitored agents/sensors on a frequent basis	Normal Business Hours	-	-	✓
Monitoring & Event Management					
Service Status	The Supplier will provide real time information on the availability of the agent/sensor through the ANS customer portal or the dashboard and relevant operating information.	24 x 7	-	✓	✓
Notifications	The Supplier will provide alerting and notification via email to a named customer contact. Email alerts will be provided for any alert that exceeds the threshold of severity 4 or severity Low.	24 x 7	-	✓	✓
Governance					
Vulnerability Scanning	Customer access to ANS vulnerability scanning through the dashboard which can be used to scan either an IP or domain level address (where appropriate licenses purchased).	24 x 7	-	-	✓
Dashboard Access	The Supplier will provide a real time dashboard that displays statistics and metrics on the operation of the ANS MDR Service	24 x 7	-	-	✓

	relating to the security posture and security activity across Customer Supported Assets.				
Service Operations					
Portal Access	Customer access to ANS customer portal providing visibility of all service-related tickets.	24 x 7	✓	✓	✓
Account Management	The Supplier will provide a named Account Manager	Normal Business Hours	-	✓	✓
Root Cause Analysis	Applicable to P1 Incidents only, following a successful resolution of a P1 Incident, the Supplier will perform Root Cause Analysis. In the case of recurring Incidents (regardless of priority) further analysis may be undertaken to identify the underlying cause. Where applicable a Service Disruption Report will be created.	Normal Business Hours	-	-	✓

There is no hard limit on the number of Incident Management support requests, but excessive usage will be queried by the Company and future requests changes may be chargeable. Daily requests for a period of greater than 10 days or a support request taking in excess of 30 minutes to complete will be chargeable. Charges for excessive usage will be calculated at our standard hourly rate.

2. Security Incident Management

A Security Incident is a pattern of potentially malicious activity that implies on identified threat to an information system, violates acceptable use policies, or circumvents standard security practices. The Supplier classifies incidents into four threat severity ratings: Critical, High, Medium, and Low.

2.1. Threat Severity Ratings

Customers will be sent real time alerts via email.

Alerts have been categorised as the following:

Levels 1 – 4: Low level events.

Expected on systems as day-to-day use. – no alerts will be provided.

Levels 4 – 6: Normal Events.

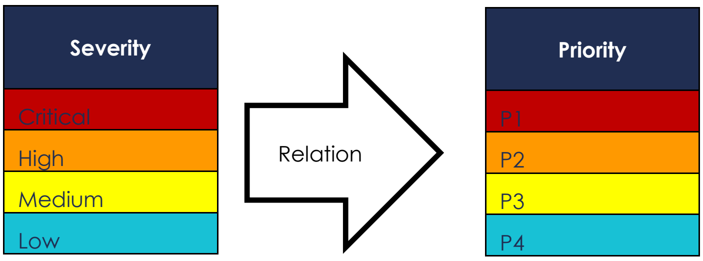
Catergorised as user activity that is expected but should be monitored. These are events such as successful logins from IPs that are expected and during normal hours, as are determined by normal custom and practices. Normal practice is determined by reference to a usual working day of 8:00am – 6:00pm.

Levels 7 – 8: High Severity Alerts.

Will need immediate investigation, such as successful logins from unknown IP addresses, change of user account permissions.

Levels 9 – 10: Critical Alerts.

Investigate immediately, indicators of a system compromise, such events as successful logins after failed attempts, modifications to core system files, modifications to payment gateway files.



2.2. Incident Response and Escalation Table

Incident Priority	Threat Severity Rating	Response SLA	Escalation Notification	Notification Type
P1	Critical	30 Minutes	Immediate	Email/Portal /Telephone Call
P2	High	1 Hour	None	Email/Portal
P3	Medium	4 Hours	None	Email/Portal
P4	Low	1 Day	None	N/A
P5	Question Query	2 Days	None	N/A

For an Incident, "Response" is the time from when the ticket is first logged within the Supplier ITSM Tool to the time that the Supplier responds with a suitably qualified Employed person whether via an email. GLASS Portal update, telephone call (dependant on Priority).

For detailed process flow see the current Managed Services Handbook. Support to provide a resolution this shall be provided within Service Hours from the time of Response until the Incident has been resolved.

From the time of Response until resolution, updates shall be provided to the Named Contacts and/or Escalation Contacts by email or GLASS Portal updates at such frequencies as set out in section 2.4.2 below.

Incident Resolution is handled by the Change Authority of the Supported Asset under investigation.

2.3. Security Incident Remediation

Remediation steps for Security Incidents are shared with the Customer by the Supplier. Resolution of and carrying out remedial steps is the responsibility of the Change Authority of the Supported Asset under investigation.

If the Supported Asset is under a Managed contract with the Supplier, then the Service Levels of that contract will comply and the Supplier will remediate via the Suppliers Change Management Process.

Where the Customer is the Change Authority then the Incident will be functionally escalated (assigned) to the Customer to deliver any required remedial actions via Change Management.

2.4. Platform Incident Management

2.4.1. Platform Incident Priority Table

Affect	Business Impact		
	Minor	Moderate	Major
System/Service Down	P3	P2	P1
System/Service Affected	P4	P3	P2
User Down/Affected	P5	P4	P3

2.4.2. Platform Incident Response and Escalation Table

Priority	Response SLA	Specialist Review	Escalation Manager	Escalation Director	Notification Frequency	Target Resolution KPI
P1	30 Minutes	1 Hour	Immediate	Immediate	Hourly Email	4 hours
P2	1 Hour	2 Hours	4 Hours	None	GLASS Portal	1 Day
P3	4 Hours	1 Day	2 Days	None	GLASS Portal	10 Days
P4	1 Day	Never	Never	None	GLASS Portal	30 Days
P5	2 Days	Never	Never	None	GLASS Portal	None

For an Incident related to the ANS MDR platform, "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 (dependant on Priority).

For detailed process flow see the current Managed Services Handbook. Support to provide a resolution shall be provided within Service Hours from the time of Response until the Incident has been resolved.

From the time of Response until resolution, updates shall be provided to the Named Contacts and/or Escalation Contacts by email or GLASS Portal updates at such frequencies as set out in the table above.

3. Service Level Targets

Category	Service Level Target
P1 Incidents	100% of Incidents responded to within 30 minutes – 24x7 Service Hours.
P2 Incidents	100% of Incidents responded to within 1 Normal Business Hour.
P3 Incidents	100% of Incidents responded to within 4 Normal Business Hours.
P4 Incidents	100% of Incidents responded to within 1 Working Day.
P5 Incidents	100% of Incidents responded to within 2 Working Days.
Root Cause	100% of P1 Incidents to receive a Root Cause Analysis within 10 Working Days of Resolution.

4. Exclusions

The following are listed as exclusions, but this list shall not be considered complete or exhaustive and the Agreement should be consulted.

For the purpose of these sections "Customer Supported Assets" means the Cloud solution provided by the Supplier to the Customer and in relation to which ANS is providing the support more particularly outlined in these Product Terms.

"Demarcation Zone" means infrastructure or solutions not being Customer Supported Assets.

a. Issues resulting from misconfiguration by the Customer outside of the Demarcation Zone resulting in impact to the Customer Supported Assets.
b. Issues resulting from failures in maintenance/administration by the Customer outside of the Demarcation Zone resulting in impact to the Customer Supported Assets.
c. Issues resulting from Unauthorised Access by the Customer of Customer Supported Assets.
d. End User or 1st Line support.
e. Technical Advice to any persons not listed as a Named Contact.
f. Failure to meet SLA due to Vendor outages.
g. Project Changes (Normal CR6) are excluded from the service and will be subject to Additional Service Charges. Project Changes are recorded within the Supplier ITSM Tool for Informational and approval purposes only.
h. Daily requests for a period of greater than 10 days or a support request taking in excess of 30 minutes to complete will be chargeable. Charges for excessive usage will be calculated at our standard hourly rate.
i. Deployment and configuration of ANS MDR outside of the Customer Supported Assets.
j. Security incident containment and/or remediation outside of the deployed ANS MDR platform is dependent on additional service contract being in place for the specific technology e.g., ANS ECloud VPC.
k. Only the service level quoted and purchased included, please refer to your signed contract.

5. Customer Responsibilities

Including but not limited to:

a. The Customer shall have an established end user support function that may be validated by the Supplier.
b. Where required, the Customer shall make available appropriately skilled Employed persons while an Incident is being managed.
c. The Customer is required to undertake an initial Impact Assessment before logging the Incident with the Supplier. Such Impact Assessment is to include:
    a. Affected Services.
    b. Business Impact.
    c. Number & Type of users affected.
    d. Recent changes on Supported Assets (regardless of perceived impact).
    e. The Customer shall check hardware onsite and ensure the hardware has power and cables are connected as expected.
    f. The Customer shall check LED status of equipment where required onsite.
d. The Customer shall provide full administrative access to the Supplier to all the services outlined in the Impact Assessment and any subsequently identified services or provide persons with adequate access to allow investigations to proceed.
e. The Customer is required to ensure that all Customer Supported Assets are appropriately licenced and have Supplier recommended hardware and vendor support in place.
f. The Customer is responsible for all configuration backups outside of the Customer Supported Assets without exception.
g. The Customer is responsible for all data and configuration backups without exception. The Supplier does not backup any Customer data.
h. The Customer is responsible for completing a Request for Change (RFC) in accordance with the Supplier's Change Management Process.
i. The Customer shall ensure that all relevant Customer employees have access to and have read the Supplier's Managed Services Handbook.
j. The Customer shall ensure an on-going availability of suitable Internet connection (if not provided by the Supplier).
k. The Customer shall ensure 24x7x365 availability of a suitable Escalation Contact should the Supplier need to gain approval for an Emergency Change or to engage other aspects of the Customer's support functions.
l. The Customer shall provide suitable notice to any planned/scheduled maintenance that could affect the Customer Supported Assets including environmental changes. Failure to do so may result in Additional Service Charges.
m. The Customer shall request permission from the Supplier in writing in the event that the Customer wishes to change the location of the Customer Assets and/or Supplier Assets from the address specified in the Contract. Any asset that has been moved without notification to ANS will be subject to additional service charges.
n. If the Customer requires the Supplier to provide onsite hands and eyes support, then this will be subject to Additional Service Charges.
o. It should be noted that the Customer shall report Business Critical Incidents via telephone only. The Supplier cannot offer any Service Levels or Service Credits for Business-Critical Incidents raised via email.
p. Configuration of source technology sending logs into ANS MDR, unless the Customer Supported Asset is under a Managed contract with the Supplier.
q. The Customer shall be responsible for any Licensing requirements.

6. Assumptions

a. All Customer Supported Assets within the Demarcation Zone within this Contract are covered by a valid software maintenance and support agreement in line with this Contract Service Levels.
b. All Customer Supported Assets are in a Valid Supported Configuration at the point of contract start date.
c. All Customer specific pre-requisites have been completed before contract commencement.
d. The Customer will provide a suitable specification platform and operating system for the Enterprise Monitoring collector server.
e. The Customer will provide resource to work with the Supplier to on-board the service.

7. Pre-Requisites

a. On-Boarding Health Check and Documentation.
b. Platform and where applicable WMI access for all monitored services.
c. Administrative Access Permissions for ANS Engineers on supported Subscriptions.
d. Registered Partner Admin Link and/or AWS Associated Partner registration (where required).

8. Partner Admin Link

ANS' Managed Cloud for Azure incorporates Microsoft Signature Cloud Support for any issues that require escalation to Microsoft. For this to be able to be fulfilled, Microsoft leverage information collected from the Partner Admin Link (PAL) system to assign back-end support rights. As such ANS must be registered as the digital PAL on any Subscriptions that contain or contribute to assets under support or management for the entire duration of the agreement. Consequently, the Customer shall, prior to the Commencement Date arrange for ANS to be registered as the PAL and must have either Owner or Contributor rights to all subscriptions and resources that contain or contribute to assets under support or management for the entire duration of this agreement.

9. Amazon AWS Associated Partner

If required, Amazon AWS' partnership status is heavily reliant on demonstrating working relationships with AWS consumers, Amazon leverage information collected from the associated partner system to assign partnership status. As such ANS must be registered as the associated partner on any accounts that contain or contribute to assets under support or management for the entire duration of the agreement. Consequently, the Customer shall, prior to the Commencement Date arrange for ANS to be registered as the associated partner on all accounts that contain or contribute to assets under support or management for the entire duration of this agreement.