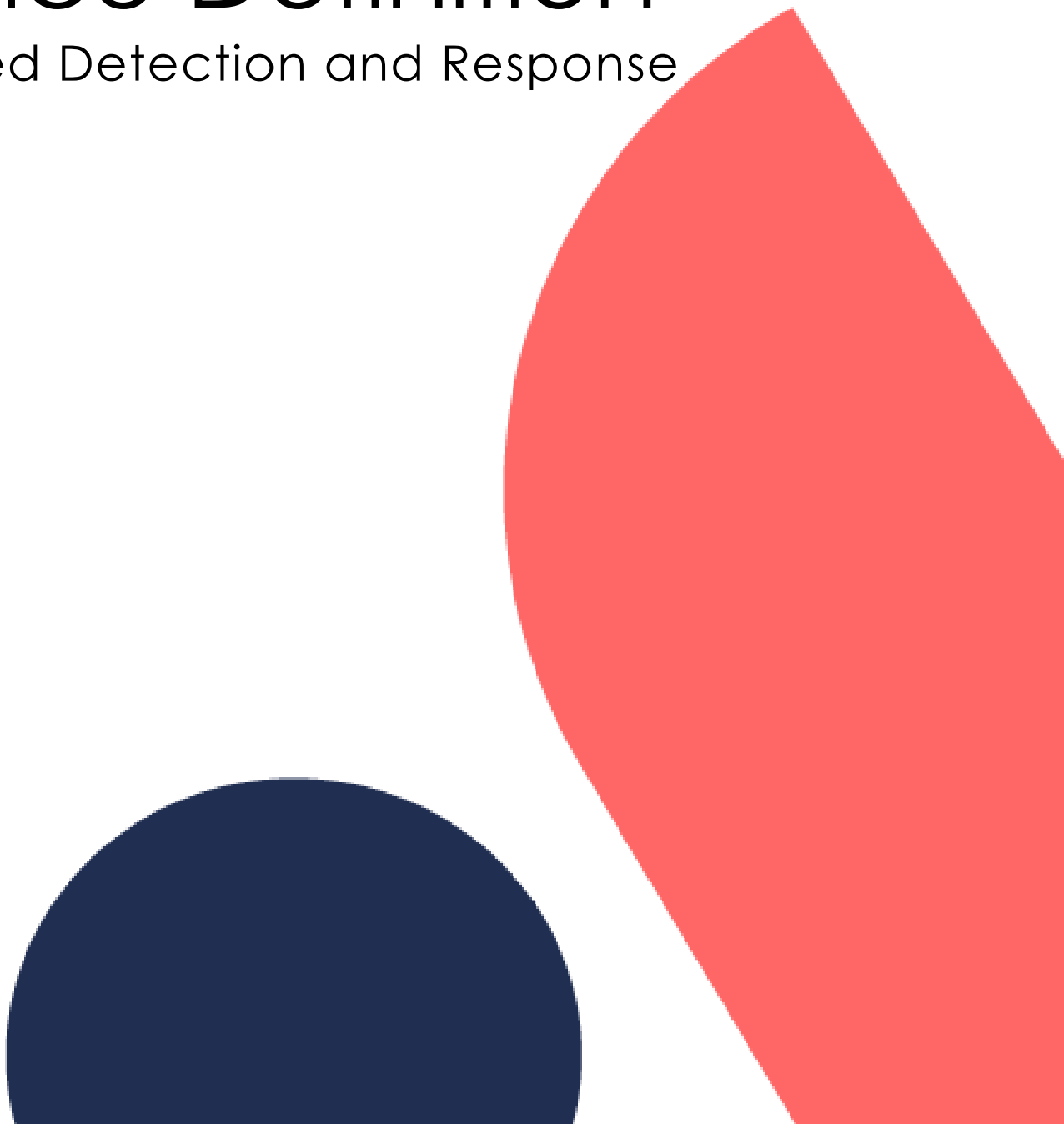
Service Definition

Managed Detection and Response



1. Operational Services

1.1. Terms and definitions

In this schedule, the following words shall have the following meanings:

Term	Definition
Normal Business Hours	09:00 - 17:30, Monday to Friday (excluding bank holidays).
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.
Working Day	8.5 Normal Business Hours.
Service Operation	The service is operated 24x7.
24x7	24 hours a day, 7 days a week.
Annex One	Means the annex to this Appendix which articulates the Scope of Services and details locations, platforms, devices and applications in scope for management by the service.
Annex Two	Means the annex to this Appendix which articulates the Service Levels associated with the service.
Customer Data	Means all data provided to the Supplier or a Supplier Affiliate by or on behalf of the Customer in connection with the provision of the Services, and includes the Customer's Personal Data.
The Customer	Means the Customer as described in the Master Services Agreement.
Customer User	Means a User within the Customer organisation identified as entitled to receive the Service, the total number of which is set out in the Service Order Schedule.
The Supplier	Means ANS Group as described in the Master Services Agreement.
Item	Means a server, device, endpoint or application source for which a vulnerability or security event can be discovered.
Security Incident	Means is 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.
Service Desk	Means the primary point of contact between the Customer Users and Supplier for all Incidents and Service Requests.
Service Request	Means 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.
The Service	Means the delivery of cyber security services defined in this document to the scope of technologies as described in this document.
Service Levels	Means any contracted service levels for this Service as specified in Annex Two (Service Levels).

Vendor	Means the owner or reseller of the third party technology and services.
Alert	Means the creation of a notification in relation to a security event that is not yet determined as malicious or harmful or a security incident.
Detection	The platform capability to detect a threat or security incident for which a response is required.
Response	Is the action taken by the Supplier to acknowledge alert/s and begin an investigation into the status of the alert/s.
Incident Response	Means 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.
Containment	The process or implementation of a defined action as part of a strategy, during the handling of a security event that aims to minimise the scope of the security event and contain the effects of unauthorised activities within the environment.
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 your organisation.
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.
Lessons Identified	Are opportunities for improvement to develop preventative controls or response actions in relation to cyber risk controls.
Remediate	Refers to the actions to reverse, stop damage, improve or correct the actions effecting the IT environment.
Service Term	Means the term for the Services as specified in the Service Order Schedule.
Vulnerability Intelligence	Consolidation of data from multiple sources giving a contextualised assessment of organisational risk arising from identified vulnerabilities.
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.
Major Security Incident	A significant Incident that has impact to multiple or critical IT systems that requires a combined, multi-team approach to resolve.
Emergency Change	An expedited Change process usually used to apply controlled IT Change usually in response to a significant incident or event.
Artificial Intelligence	Computer systems able to perform tasks normally requiring human intelligence.

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.
Vulnerability Scanning	Assessment of the organisations assets in relation to known vulnerabilities.
Malware	Software or applications that seek to disrupt, damage, or gain unauthorised access to a computer system and compromise the organisation's operational functions.
SOC Analyst	An analyst working in the Security Operations Centre with security based technical skills who can analyse the data surrounding a security event and apply the appropriate response to ensure Confidentiality, Integrity and Availability of the Information System.
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 evaded existing security solutions.
Dark Web scanning	The "dark web" consists of hidden websites that cannot be accessed without special software. This scanning checks to see if sensitive organisational or personal data can be found on the "dark web".
Service Availability	Measure of the service being available and accessible to the Customer during the time the Supplier promises to keep the service available.
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.
Co-Managed	A partnership between the Customer and the Supplier to manage tooling, where the Supplier brings subject matter expertise to support effective operations.
Fully-managed	Outsourcing the management and delivery of technical systems to a Supplier partner.

2. Overview

The Supplier's Managed Detection and Response (MDR) Service is designed to provide the right level of response to meet the Customer's needs, ultimately better securing their business. The service is delivered through a partnership defined by the Supplier to meet the cyber security needs of the Customer.

2.1 A summary of the Service is as follows:

2.1.1 provision of a Security Operations Centre (SOC) 24/7.
2.1.2 trained Security Analysts and Engineers.
2.1.3 detection rule and process management.

2.1.4 alert triage and assessment with threat intelligence.
2.1.5 security analysis with customer business contextualisation.
2.1.6 threat Detection and Response.
2.1.7 Incident Response and Containment.
2.1.8 Security Incident Management, with appropriate advice and guidance.
2.1.9 Telephone and email support.
2.1.10 Early value realisation through Supplier accelerated onboarding.

3. Scope

The scope of this Service is set out in supported devices list (Annex One):

3.1 The Supplier will provide a Managed Security Service that will:

3.1.1 Deploy (where applicable) and manage the Customers Microsoft Security products, as listed in Scope of Services.
3.1.2 Configure relevant correlation rules, security related asset tagging and security settings.
3.1.3 Manage the alert signals and proactively tune the system to reduce false positives.
3.1.4 Manage the data flow into the environment to enable cost efficiency and reduce cost of tool operation.
3.1.5 Monitoring of the named Microsoft security platform for operational performance and availability.
3.1.6 Provide management of the security tooling during normal business hours.
3.1.7 Provide monitoring of the security platform 24/7.
3.1.8 Provide Access Control for all Supplier staff required to deliver the service.
3.1.9 Provide a secured Security Operations Centre (SOC) facility with operational resilience for business continuity.
3.1.10 Provide trained SOC analysts and other relevant staff to manage the scope of service delivery.
3.1.11 Provide a SOC facility with Supplier staff based in the United Kingdom.
3.1.12 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.
3.1.13 Conduct service reviews on a quarterly basis to discuss the quality-of-service delivery and address any service issues.
3.1.14 Produce monthly reporting in the form of a dashboard to display relevant events occurring due the delivery of service.
3.1.15 The Customer may test the service once, post the full completion of onboarding. The Supplier requires 10 working days' notice for the test. The full results of the test must be shared with the Supplier for improvement and correction. Any subsequent testing is a chargeable event. All testing is subject to customer expense.

3.2 Provide a managed threat detection and response that will:

3.2.1 Develop detection rules and other capabilities and manage them as part of the service.
3.2.2 Receive an alert signal from the in scope security tooling.

3.2.3 Provide investigation and triage on all Alerts with skilled security analysts and have the unique Customer context applied.
3.2.4 Analyse the alert and assess its status in relation to positivity (True-Positive/False-Positive).
3.2.5 Use Threat Intelligence information from various sources as part of alert analysis and event enrichment.
3.2.6 Close the alert and identify as false and refer for tuning analysis, where the alert is a false-positive.
3.2.7 Raise a security Incident and associated service ticket in the ITSM tool where the alert is a true-positive.
3.2.8 Conduct an investigation of the security events generating the alerts to determine the nature and status of the events.
3.2.9 Create a security incident and commence Incident Response procedures, where the security event is malicious or potentially harmful.
3.2.10 Notify Customer named representatives via agreed channels.
3.2.11 Provide security notification 24/7.
3.2.12 Provide classification using the MITRE ATT&CK framework to classify various activities. The classification will be automatic and set against Microsoft security tooling and the Suppliers chosen security platform.

3.3 Provide Incident Response that will:

3.3.1 Provide an Incident Response based off Alerts generated by the Customers' existing 3rd party security providers and use the 3rd parties automated technical tooling analysis and collection to respond to suspicious security events detected within the Customer IT infrastructure.
3.3.2 Provide an investigation of the security events generating the Alerts, analyse the data and provide a security response through appropriate containment, eradication and recovery strategies applicable to the event. The response will include remediation guidance to the customer and the Supplier operational support and resolver teams.
3.3.3 Provide Containment and Eradication responses to the detected threats which follow appropriate industry recognised models (NIST, NSCS, SANS).
3.3.4 Initiate Containment actions at the first indication of suspected or actual malicious behaviour. The Supplier must be enable to do this with the Customers tooling.
3.3.5 Provide a response which supports basic root cause investigation.
3.3.6 Undertake all reasonable endeavours to deliver a containment response in a timely manner.
3.3.7 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.

3.4 Provide Incident Management that will:

3.4.1 Provide a service that covers Incident Management activities and helps coordinate the relevant resolver groups to remediate the security event or issue in line with the current contracted services.
3.4.2 Initiate response to detected Security Alerts and Incidents, as defined within the Supplier Schedule Two (Service Levels).

3.4.3 Provide Priority 1 Security Incident reporting post a Security Incident where the Supplier will within ten (10) working days produce a basic report detailing the timeline of the Incident along with any known root cause and preventative measures.

3.4.4 Provide adherence to standard contracted Supplier process for Service Request, Incident, Change and Problem Management underpinned by the Supplier's IT Service Management tooling.

3.4.5 Provide Emergency Change guidance as required to remediate Cyber Security Incidents and in the event of a significant and/or destructive Cyber 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.

3.4.6 Provide Cyber Security Incident communication throughout Incidents. The frequency of communication may vary depending on the severity of the Incident.

3.4.7 Provide bridging/conference capabilities, using Supplier provided tools, and establish calls where multiple parties (including third parties) are required to support the remediation of an Incident.

3.4.8 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 cost.

3.4.9 Provide Security Incident process initiation and management. Adhering to the Suppliers standard Cyber Security Incident Management processes, this Service includes investigation, assessment, communication, containment and mitigation advice to resolve and/or preventative threats and attacks (subject to scope of the Managed Services provided, otherwise Professional Services may be available at an additional charge).

3.4.10 Provide support to eradication and/or remediation actions and activities required to resolve security incidents within scope of the MDR Service and wider Customer contracted service for support. Any support required outside of the contracted services (design change or unsupported infrastructure), will be referred to the Customer with options for consideration. This may involve additional project work or Professional Services at additional cost to the Customer.

3.4.11 Not proceed without Customer authorisation where additional costs are to be raised. The Customer will hold all liabilities in this event.

3.4.12 Not include Digital Forensic Analysis where Incident Management is provided. Advice and guidance will be provided on selection of specialist 3rd party expertise.

3.5 Provide Threat Hunting that will (where the Customer has contracted Threat Hunting services):

3.5.1 Provide a service that will proactively search for indications of malicious activities not identified by the security tooling.

3.5.2 Use the data collected by the security tooling as the source of data for searching. Devices and Information Systems not covered by the Customers security tooling are excluded from threat hunt searches.

3.5.3 Conduct Threat Hunting in the Customers provision of Microsoft Sentinel SIEM and the Customer will have a valid licence with 90 days of searchable content as minimum.

3.5.4 Use identified Indicators of Compromise (IoC) from various Threat Intelligence providers, as the primary basis for searches. This will cover known threat actors groups and their associated techniques, tactics and procedures (TTPs).
3.5.5 Conduct threat hunts on threats identified against the Customers Industry, identified Advanced Persistent Threats (ATP) targeting the UK, relevant TTPs that are in use against UK organisations.
3.5.6 Conduct threat hunts on a monthly basis and provide a report to the Customer on the search scope and findings.
3.5.7 Provide trained security analysts to undertake the Threat Hunting.

3.6 Provide a Supplier Security Platform that will:

3.6.1 Provide its own Security Orchestration, Automation and Response (SOAR) capabilities. The technology used will be at the Supplier's discretion for best service.
3.6.2 Take identified data feeds from Customer tooling to enrich and manage through the Supplier defined processes.
3.6.3 Apply additional Threat Intelligence augmentation to alert and events in the Suppliers Security platform for analysis in the platform.
3.6.4 Correlate multiple events in the Security platform.
3.6.5 Manage each individual Incident Case in the Security platform.
3.6.6 Provide Customer specific response playbooks/runbooks that are developed and used with in the Security platform.
3.6.7 Use at its discretion, automated processes in the Security platform to speed up the threat analysis, response and containment to counter cyber threats in the Customers scope of service.
3.6.8 Use the Security platform to enable best practice collaboration with the Customer, including transparency over full case history, information shares, and documentation of response activities.
3.6.9 Use the Security platform to track and measure performance, at the Suppliers discretion.
3.6.10 Provides Data segregation that is managed in the platform. A Customer specific environment will be created which will contain all Customer data. Only designated staff from the Supplier will have access and limited access will be provided to the Customer.
3.6.11 Provide Data residency in the United Kingdom. Data is held in Google Data Centres (europe-west2) based around London, UK.
3.6.12 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.
3.6.13 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 Platform will be reported to the Customer.
3.6.14 Provide a security Platform that is configured to ensure high-availability.

3.7 Provide Threat Intelligence that will:

3.7.1 Support the Customers Microsoft Security products which hold a threat intelligence feed that is native to the tool. This can be enhanced through Microsoft. The Supplier is not responsible for this provision of this threat intelligence.
3.7.2 Enrich the alert data received from the security tooling provided by reputable threat intelligence provider feeds.
3.7.3 Be from multiple sources and is at the Supplier discretion on selection.
3.7.4 Consider any additional feeds requested by the Customer and must be technically interactable with the Suppliers technology platform. The Supplier is under no obligation to accept additional threat feeds. Customers may be subject to additional charges for integration and management.
3.7.5 Support Customers defined as part of Critical National Infrastructure (CNI) including any CNI threat intelligence feeds, subject to an additional onboarding and maintenance cost.

3.8 Provide Communication channels with the SOC:

3.8.1 Provide telephone contact for normal work activities.
3.8.2 Provide email communications for normal working activities.
3.8.3 Provide an IT Service Management tool.
3.8.4 Provide teleconferencing via Supplier tooling.

3.9 Provide a response level according to severity that will:

3.9.1 Respond to event Alerts classified as Critical or High by the technology within 15 minutes of being notified. This will be provided 24 hours per day, 365 days. Events assessed as being True-Positives will be given Priority 1 (P1) status and logged in the IT Service Management tool and communicated to the Customer.
3.9.2 Respond to event Alerts classified as Medium by the technology within 4 hours of being notified. This will be provided 24 hours per day, 365 days. Events assessed as being True-Positives will be given Priority 2 (P2) status and logged in the IT Service Management tool and communicated to the Customer.
3.9.3 Respond to event Alerts classified as Low by the technology within 1 working day of being notified. This will be provided 24 hours per day, 365 days. Events assessed as being True-Positives will be given Priority 3 (P3) status and logged in the IT Service Management tool and communicated to the Customer.
3.9.4 Provide a major incident report on verified P1 incidents within 10 working days of the closure of the Response.
3.9.5 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.
3.9.6 Consider any automated response to an alert or incident as a response in relation to the SLAs previously stated.
3.9.7 All have all Alerts and Incidents reviewed by the Suppliers trained security analysts.

4. Hours of service

4.1 Normal office hours are 9am to 17:30pm Monday to Friday (excluding UK Public Holiday).

4.1.1 Detection and Response service is available 24 hours a day, 365 days per year.

5. Boundaries

5.1 The Supplier does not provide vendor integrated Digital Forensic Response retainer Services.

5.1.1 Work done by the Supplier on the Customers environment remains the intellectual property of the Supplier.

5.1.2 The Supplier does not share any intellectual property created in support of the service with the Customer.

5.1.3 The service is not an IT Operational service monitoring or problem identification service and is not responsible for IT operational under performance issue identification.

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

6. 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 15 minutes.	100%	A Service credit will be offered in the following way, 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 4 Hours.	Service credits apply from 2nd failure within a calendar Month	A Service credit will be offered in the following way, 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;

P3 Incidents or lower	100% of Incidents responded to within 1 Working Day.	None	No 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; the Service will commence once the Microsoft Security tooling has been onboarded to the Suppliers Security platform and the Supplier is Detecting and Responding to Alerts from the Customers environment.

7. Customer Responsibilities

7.1 The Customer will:

7.1.1 Provide the Supplier with technical access and relevant permissions to deliver the service under the scope of service, including providing the Supplier with authorisation and technical access to enable automated response for Containment and threat hunting. This includes the provision of Azure Lighthouse accounts in Microsoft tooling and access to other security tools in scope.

7.1.2 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.

7.1.3 Assist the Supplier in the remediation of issues that may prevent operation of this Service.

7.1.4 Will 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.

7.1.5 Submit all service requests to the Supplier Service Desk, by means of the telephone or electronically by one of the designated named Customer's contacts.

7.1.6 Attend regular meetings scheduled at mutually convenient times.

7.1.7 Inform the Supplier, with a minimum of 5 working days, of any change that may impact the operation of the service.

7.1.8 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.

7.1.9 Update the Supplier of changes to nominated individuals and associated contact details.

7.1.10 Support the Supplier with timely decision making in order to enable the appropriate countermeasures to a security incident to be deployed or enacted.

7.1.11 Will not hold the Supplier liable for any highly sophisticated or advanced threat actor attack that may occur that goes undetected by the tooling.

7.1.12 Will not hold the Supplier liable for any impacts of a malicious attack by any third party or malicious insider.
7.1.13 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. Standard Rate Card will apply.
7.1.14 Acknowledge and respond to incidents escalated by the Supplier with individuals nominated by the Customer to be included in the security event notification process.
7.1.15 Provide reasonable availability of Customer representative(s) when resolving a security related incident or request.
7.1.16 Ensure that all Customer Supported Assets are appropriately licensed and have Supplier recommended hardware/software and vendor support in place.
7.1.17 Ensure an on-going availability of suitable Internet connection (if not provided by the Supplier).
7.1.18 Report Business Critical Incidents via telephone only. The Supplier cannot offer any Service Levels of Service Credits for Business-Critical Incidents raised via email.
7.1.19 Configure source technology to send logs into Microsoft Sentinel, unless the Supported Asset is under a managed contract with the Supplier.
7.1.20 Pre-authorise the Supplier to make changes to the Detection ruleset and policies without going through change control or Customer signoff. 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.
7.1.21 Acknowledge any changes by the Customer that disrupt the service will be subject to additional charges, at the standard rate card, to rectify and remediate.
7.1.22 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.

8. Assumptions

8.1 All Customer Supported Assets and Azure Accounts within the Supported Assets within this Contract are covered by a valid software maintenance and support agreement in line with this Contract Service Levels.
8.2 All Customer Supported Assets are in a valid supported configuration at the point of contract start date.
8.3 All Customer specific pre-requisites have been completed before contract commencement.
8.4 The Customer will provide a suitable specified platform to host the secured operating system for the Enterprise Monitoring collector server.
8.5 The Customer will provide resource to work with the Supplier to on-board the service, and assist with maintenance tasks as required.

9. Pre-Requisites

9.1 On-Boarding Health Check and documentation.
9.2 Deployment of Supplier's accelerated Microsoft Sentinel deployment to agreed scope, defined in Statement of Work.
9.3 Platform and access for all performance monitored services.
9.4 Administrative access permissions for Customer Engineers on supported subscriptions.

10. Exclusions

The following are listed as exclusions to this service:

Note – this list shall not be considered complete or exhaustive and the **Terms and Conditions** should be consulted:

10.1 Issues resulting from misconfiguration by the Customer of the supported assets and scope of service, resulting in impact to the Service.
10.2 Issues resulting from failures in maintenance/administration by the Customer of the scope of service resulting in impact to the Service.
10.3 Issues resulting from Unauthorised Access by the Customer of the scope of service.
10.4 Issues created by the Customer on systems that affect the scope of service that impact the ability for the Supplier to deliver the service.
10.5 End User or 1st Line support.
10.6 Technical advice to any persons not listed as a Named Contact.
10.7 Failure to meet SLA due to Public Cloud provider outages.
10.8 Project Changes 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.
10.9 Emergency Changes that are not a direct output of a Priority 1 incident may be subject to Additional Service Charges.
10.10 Deployment and configuration of Log Analytics Workspace, Microsoft Sentinel, Data Connectors and Workbooks outside of the scope of service.
10.11 Provisioning and configuration of any Infrastructure or Operating Systems required to host Log Forwarders and Sentinel Platform components outside of the scope of service.
10.12 Security incident containment and/or remediation outside of the deployed Sentinel platform is dependent on additional service contract being in place for the specific technology.
10.13 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.
10.14 The Customers technology failing to respond to an execution command initiated by the Supplier to a Containment activity.

11. Annex One – Scope of Services

The scope of Service covered in this agreement:

- Assets
- Priority Systems and Assets
- Key Personalities
- Network Address ranges (Internal and External)
- Registered Domains
- Identified Industries of operation

12. Annex Two – Service Levels

The Supplier will ensure that Security Incidents are managed and responded to as per the below Service Level(s). These Service Levels apply to the Security Incident response commitments for all types of information Security Incidents. Incident response times vary according to the Priority Level assigned to the Incident.

Security Incident Priority	Response	*Containment	Escalation
Priority 1: Critical & High	15 mins (24/7)	24/7 containment response based on reasonable endeavours to contain. Eradication based on normal working hours.	SOC Manager Director of Security Operations
Priority 2: Medium	4 hours (24/7)		SOC Manager Director of Security Operations
Priority 3: Low	1 Business Day (24/7)		SOC Manager