1. Service Overview

Our Managed Cyber Security Service is provided by our Security Operations Centre (SOC) centre, which leverages a Security Information Event Management (SIEM) platform to monitor and manage your infrastructure.

Our SOC analysts work to isolate and contain threats using Microsoft Defender technologies that ingest directly to a centralised SIEM platform.

The Managed Cyber Security Service leverages a choice of Service packages. These are:

(a) Managed Detection and Alert (MDA);

(b) Managed Detection and Response (MDR); and

(c) Managed Extended Detection and Response (MXDR).

We will consult with you to help you choosing the Service package that meet your requirements, and we will document your choice and the associated Fees in your Order Form and/or Statement of Work (SoW).

2. Solution Overview

Our Service can be provided on the following Microsoft Defender platforms:

(a) **Microsoft Defender for Endpoint** is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

(b) **Microsoft Defender for Identity** is a cloud-based security solution that helps secure your identity monitoring across your organization. Defender for Identity is integrated with Microsoft Defender XDR, and leverages signals from both on-premises Active Directory and cloud identities to help you identify, detect, and investigate threats directed at your organisation.

(c) **Microsoft Defender for Office 365** offers integration into Microsoft 365 subscriptions to reduce the risk of threats in email, links (URLS), file attachments, and collaboration tools.

(d) **Microsoft Defender for Cloud Apps** is designed to improve the protection of SaaS applications, helping you monitor your cloud app data across the cloud access security broker (CASB), Self-Service Password Management (SSPM).

(e) **Microsoft Defender for Cloud** is a cloud-native application protection platform (CNAPP) made up of security measures and practices that are designed to improve

protection of cloud-based applications. Defender for Cloud combines both Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) capabilities.

(f) **Microsoft Entra ID Protection** helps organizations detect, investigate, and remediate identity-based risks.

(g) **Microsoft Sentinel** is Microsoft cloud-native security information and event management (SIEM).

(h) **ServiceNow** is the incident management system (IMS) that we use to manage tickets and SOC resources.

Please note that we will provide the Service for the various Microsoft Defender platforms where you have the relevant platforms in place, and such platforms has been included in the scope of the Statement of Work as agreed with you. If you do not have the platforms or the required licensing in place, we can offer professional services at an additional Fee for the setup and provisioning of these platforms, which can be scoped into the Statement of Work where required.

3. Service Packages

As part of this Service, we offer three different packages: Managed Detection and Alerting (MDA), Managed Detection and Response (MDR), and Managed Extended Detection and Response (MXDR). Each Service package offers a tailored approach to incident response:

(a) MDA focuses on alerting to potential threats, whilst you remain responsible for the response actions;

(b) MDR provides additional investigation and response capabilities for incidents on your endpoints;

(c) MXDR extends the scope of MDR by incorporating response capabilities to provide the Service across Defender for Endpoint, Defender for Identity, Defender for Office 365, Defender for Cloud Apps, Defender for Cloud and Entra ID Protection.

Your Service and the associated Fees will be defined in your Order Form and/or SoW.

3.2 Managed Detection and Alert (MDA)

Our Managed Detection and Alert (MDA) Service package leverages the technologies described in Section 2 to monitor your digital environment. When an alert is generated, our SOC will conduct an analysis to understand the nature and severity of the potential threat. While we don't directly intervene, we will provide you with detailed response guidance, including steps that you should take for recovery and recommendations for post-incident review.

Key features:

(a) Monitoring technology;

(b) Analysis of security alerts;

(c) Response guidance provided by our SOC; and

(d) Guidance for recovery and post-incident review provided by our SOC.

3.3 Managed Detection and Response (MDR)

Building upon the MDA foundation, our Managed Detection and Response (MDR) Service package extends our capabilities to your endpoints, specifically utilising Defender for Endpoint. In addition to analysing alerts, we will attempt to contain and eradicate incidents on your endpoints. Our SOC team will also provide you with instructions for recovery and guidance that you can follow to review the incident.

Key features:

(a) Includes all MDA Service package features;

(b) Response capabilities to assist with containment and eradication of incidents on endpoints;

(c) We will leverage your Defender for Endpoint technology; and

(d) Recovery instructions and review guidance provided by our SOC.

3.4 Managed Extended Detection and Response Service (MXDR)

Our Managed Extended Detection and Response (MXDR) Service package provides incident response capabilities across the range of technologies as described in Section 2 within the terms of engagement that we will agree with you and document in your Low-Level Design document. MXDR can leverage Defender for Endpoint, Identity, Office, Cloud Apps, Cloud, and Entra ID, as well as alerting for any technology integrated into Sentinel that we cannot natively respond to. For alerts beyond these specified technologies, we will follow the MDA approach and provide analysis and response instructions, whilst you remain responsible for the performance of the response activities.

Key features:

(a) Incident response across your Microsoft Defender technologies included in the scope of your Service (as specified in your SoW) and Entra ID Protection;

(b) Analysis and response guidance for alerts from technologies integrated into Sentinel; and

(c) Threat containment and eradication capabilities as described in this Service Description.

3.5 Threat Intelligence

As part of this Service, we use threat intelligence to correlate entities and investigate their historical context, as well as to stay up to date with the latest cyber security news.

Please refer to our separate Threat Intelligence Service Description if you wish to procure additional Threat Intelligence capabilities and receive weekly and monthly reporting about industry sectors, personalised visibility on the latest threats and vulnerability exploits.

4. Response Capability Per Service

Our response capabilities vary across different Service packages as described below:

(a) **Analysis:** as part of all Service packages (MDA, MDR, MXDR), we will perform identification and investigation of potential threats, leveraging the integrated capabilities of our security stack. The analysis phase is critical in determining the nature and scope of the threat, informing subsequent response actions.

(b) **Contain:** the capability to contain a threat is available as part of the MDR and MXDR Service packages. Containment actions are designed to limit the spread of an incident within the environment. This may involve isolating affected systems, blocking malicious network traffic, or temporarily disabling compromised accounts. If you are procuring MDA, we will provide you instructions on how to perform containment activities, but these will remain your responsibility and will not be carried out by ourselves.

(c) **Eradicate:** provided as part of the MDR and MXDR Service packages, eradication involves attempting the removal of threats from the environment. This could include the deletion of malicious files, removal of unauthorized access, and remediation of vulnerabilities that were exploited during the incident. If you are procuring MDA, we will provide you instructions on how to perform eradicate activities, but these will remain your responsibility and will not be carried out by ourselves.

(d) **Recover:** recovery actions, such as restoring systems to normal operation and ensuring that affected services are returned to a secure state, are not included in the scope of the Service. This is because IT systems are managed independently by yourself, and we will not have the capacity to perform recovery. We will provide you guidance in the form of an initial set of guidelines for the recovery steps, and, upon request, documentation related to the performance of recovery activities.

(e) **Review:** post-incident review processes are not included in the scope of the Service. If you perform your own review, leveraging insights and data provided by our team during and after incident response, we will, where possible, use the information that you provide us to address gaps to the incident process in accordance with your requirements.

Service Matrix

Below is a summary of the actions that we will perform as part of each Service package:

NIST aligned action	MDA	MDR	MXDR
Analysis	Yes	Yes	Yes
Contain	No	Yes	Yes
Eradicate	No	Yes	Yes

Recover	No	No	No
Review	No	No	No

4.2 Response Capability Per Technology

The level of response capability varies depending on the technologies that you have in place and the Service package that you are procuring from us. Below is an expanded view of what each technology offers in terms of response capabilities under MDA, MDR, and MXDR services:

(a) **Defender for Endpoint:** under MDR and MXDR services, Defender for Endpoint enables active response actions, including threat containment and eradication on endpoints as described in Section 4(c).

(b) **Defender for Identity:** this technology offers response capabilities under the MXDR Service package. It facilitates the detection and response of identity-based threats for user accounts that are protected under the Defender for Identity product.

(c) **Defender for Office 365:** available as part of MXDR Service package, Defender for Office 365 provides capabilities to respond to threats against email and collaboration tools. This includes actions to address phishing, malware, and other email-based threats.

(d) **Defender for Cloud Apps:** response capabilities for this technology are available as part of the MXDR Service package. This technology facilitates the control and mitigation of threats within cloud applications, including sanctioning/un-sanctioning apps, controlling data travel, and enforcing compliance policies.

(e) **Defender for Cloud:** available as part of the MXDR Service package, Defender for Cloud offers response capabilities across cloud workloads. By default, our response actions will only be performed subject to your prior permission as Defender for Cloud assets are typically mission critical and highly important for day-to-day operations (e.g. databases, containerised applications, repositories etc.). Our default response includes proactive recommendations from Defender for Cloud to help you secure your estate.

(f) **Entra ID Protection:** this technology is available as part of the MXDR Service package to enhance identity security by providing additional protection features such as risk-based conditional access, detection of identity-based threats, and automated mitigation actions to mitigate the risk of compromised identities. It also provides functionality to block user accounts and reset user passwords which you can use to verify or drop high risk sign-ins and user activities.

(g) **Azure Logic Apps:** available as part of both the MDR and MXDR Service packages, Azure Logic Apps is tightly integrated with Azure Sentinel to enable automated and customisable response capabilities tailored to your environment. Logic Apps enables response workflows that address specific incident types and actions, providing an automation layer for streamlined response, containment, and remediation. These response workflows include:

(i) **Automated threat response**: when Sentinel generates alerts, Logic Apps initiate predefined workflows to execute automated responses, such as isolating compromised devices in Microsoft Defender, restricting access in Azure AD, or blocking suspicious IP addresses in the firewall;

(ii) **Incident management**: Logic Apps can trigger notifications, escalate critical alerts to SOC analysts, or create tickets in Jira Service Management, facilitating the tracking, management and escalation of incidents in line with defined Service Level Agreements (SLAs);

(iii) **Enrichment and validation**: Logic Apps workflows offer additional external threat intelligence sources for Sentinel alerts, such as VirusTotal, Azure Threat Intelligence, and customer-specific data sources, providing context that supports SOC analysts in making informed decisions; and

(iv) **Compliance and audit trail**: Logic Apps workflows provide a detailed, auditable trail of automated actions, enhancing transparency and supporting compliance with standards like GDPR, PCI-DSS, and ISO27001 by maintaining detailed records of automated actions and response processes.

Through the execution of these automated response capabilities, Logic Apps is designed to improve response times and to reduce operational overhead, which allows the SOC to focus on high-priority, complex incidents that require human intervention.

Response Per Technology Matrix

Below is a summary of the technologies that you may include in the scope of each Service package:

Technology	MDA	MDR	MXDR
Defender for Endpoint	No	Yes	Yes
Defender for Identity	No	No	Yes
Defender for Office 365	No	No	Yes
Defender for Cloud Apps	No	No	Yes
Defender for Cloud	No	No	Yes
Entra ID	No	No	Yes

5. Service Package Features

As a standard, our Services includes the features listed in the table below. Any additional feature that you may require must be mutually agree and documented in your SoW and in your Service Configuration Document.

Technical Feature	Description
24x7 security monitoring	We will monitor your environment 24x7. Our Security Operations Centre (SOC) provides round-the-clock coverage to identify and respond to potential security

	incidents in accordance with this Service Description and the targets set out at Sections 13 and 14.
Log analysis	We will retain SIEM data for a minimum of ninety (90) days by default, with the option to extend retention to meet compliance or investigative needs. Please note that longer retention periods may be subject to an additional Fees. We recommend extending this default to a minimum of one year. Logs are securely stored within the SIEM, enabling our analysts to search across data sources to analyse potential threats and support ongoing investigations.
Threat detection	Our threat detection capabilities combine user and entity behaviour analytics (UEBA), analytics rules, cross-log source correlation, and our custom rules to monitor suspicious behaviour across your environment, correlate data from various log sources, and apply tailored detection rules.
Threat response	When our SOC detect a potential incident, we will analyse and respond by containing and eradicating incidents from assets managed in Defender XDR, as described in this Service Description. Where you have marked your devices or identities as 'mission critical', we will not directly respond without your prior consent.
Threat hunting	We conduct proactive threat hunting to attempt the identification of emerging threats that may evade automated detection. If our threat intelligence platforms highlight new vulnerabilities or attack patterns, our SOC analysts will initiate hunts across your environment and examine data for hidden indicators of compromise.
Incident triage & SLA	We will perform incident triage to review, assess, and prioritise incidents according to their potential impact. We will classify incidents into priority levels (P1, P2, and P3) with associated response times and escalation needs in accordance with Sections 13 and 14. We may adjust the incident priority following our investigation in line with the severity of the incident.
Emergency notifications	We will notify your designated contacts when critical severity (P1) security incidents,, are detected. We will send you the initial notification via email and phone call whilst we perform our analysis, and provide you a summary of the incident, including the severity level, potential impact, and recommended actions.
Proactive security monitoring	Our Service include monitoring of your environment for signs of unusual activity, potential threats, and emerging vulnerabilities.
Dashboards & reporting	Our dashboards and reporting capabilities provide visibility into your security landscape with customisable workbooks in Microsoft Sentinel. These workbooks are designed to give you insight into key metrics, threat detections, and incident trends. As part of the Service, we will give you access to our customer portal where you will be able to review analytics on SOC performance, including incident and threat performance metrics. Please refer to Section 15 for more information on how to request changes to your workbooks.
Custom detection rules	You can request custom detection rule creation through our customer portal. Changes to custom detection rules are subject to Section 15. We will use Microsoft Sentinel's rule-building capabilities to develop bespoke detection rules designed to identify specific indicators of compromise (IoCs) and behaviours in line with your requirements. Please note that this is not a formal detection engineering engagement. For more extensive or complex rule sets and connectors, a separate scoping and engagement may be required, as these are outside the standard Service.
In-life tuning	We will perform tuning of your environment in accordance with our standard practice during Service Implementation of the Service. Where benign positives and false positives are identified on the Service platform, we will perform additional tuning. Please note that we reserve the right to tune your environment as we deem appropriate, for example, by removing noisy incidents which may cause a detriment in the SOC. We will provide information about the tuning changes that we make in a tuning ticket and will notify when tuning actions have occurred.
Security monitoring and notification	Incidents are automatically generated by correlating log data 24x7. We will send notifications to your nominated contacts in accordance with Sections 13 and 14. The nominated contact(s) may include your own internal support team, a third-party support team or our internal support team.
Security orchestration, automation	Our SOAR capabilities provide automated response and orchestration for your in-scope endpoint devices, streamlining threat response through intelligent decision-making. During Service Implementation, we will deploy baseline automation rules and logic apps, enabling detection and alerting capabilities. Throughout the term of your

and response (SOAR)	Service, we will review and refine these automation rules to adapt to evolving threats and changes in the security landscape.

6. Service Management Features

The service management features described in this Section are included in the scope of all Service packages of our Managed Cyber Security Service (MDA, MDR and MXDR).

Service Management Feature	Description
Managed Services Operations Document (MSOD)	The MSOD document includes details of your relevant contacts and information on how you can contact our SOC. This document provides us with the relevant information for who to contact in case of emergency, who to raise tickets to, and who has access to our systems. Please note that you are responsible for requesting changes to your contact details in accordance with Section 15. Every time that you receive a phone call from our SOC, you will be required to provide your pin before any incident details can be disclosed to you.
Service portal	Our dedicated customer portal provides 24x7 access to manage and monitor your Service. Through this portal, you can log and view incidents, submit service requests, and access real-time dashboards and reports on SOC performance and security metrics. Additionally, the portal includes a knowledge base covering topics on SOC operations, product updates, threat intelligence insights, and security best practices. For communications relating to high-impact or critical incidents, we recommend contacting our service desk directly via phone to ensure prompt response. The portal serves as a central hub where incidents can also be raised, giving you tools and insights to assist with your security operations.
Service reports	Our service reports provide visibility into your security operations and insights into incident trends, response times, threat detections, and SOC performance metrics. Our service reports will also enable you to track key performance indicators.
Service review	We will conduct service reviews to assess the performance of the Service, review open incidents, discuss any adjustments to detection and response protocols with you and, where possible, identify potential improvements.
Quarterly business review (QBR)	We will hold quarterly business reviews sessions to present a summary of the previous quarter's security activities, including key achievements, incident analyses, threat landscape updates, and any recommendations for future improvements that we may identify. QBRs also offer an opportunity to discuss emerging security priorities with you.

7. Client Obligations

We will provide the Managed Cyber Security Service subject to the following dependencies:

7.1 Client Obligations

(a) You must not, at any time during the term of the Service, remove our access from your systems, provide access to any third party or disclose any of our confidential information or Pre-Existing IPR without our prior written consent;

(b) You are responsible for providing us with the access rights described in Sections 7.2, 7.3 and 7.4 below.

(c) You are responsible for obtaining and maintaining all licences required to enable the provision of the Service, including all relevant Microsoft licences and the licences for the

Microsoft Defender technologies listed in Section 2 that you wish to include in the scope of the Service. Please note that you can procure these licences directly from Microsoft, from a third-party provider or, subject to an additional Fee, from us as part of this Service.

7.2 Dependencies

You are responsible for providing us with the access rights set out below:

Service Tier	Defender for Endpoint	Defender for Identity	Defender for Cloud Apps	Defender for Office 365	Defender for Cloud
MDA	Access to view	Access to view	Access to view	Access to view	Access to view
MDR	Access to respond	Access to view	Access to view	Access to view	Access to view
MXDR	Access to respond	Access to respond	Access to respond	Access to respond	Access to respond

To be able to manage and respond to security incidents, our SOC requires full visibility into and access to all Defender XDR technologies listed in the table above.

It is your responsibility to grant and maintain the permissions listed in this Section 7.2, including assigning the **'MSP Approver'** role to us at the start of the project. If these permissions are not provided, our SOC's ability to support your environment will be limited, and we will not participate in your calls to troubleshoot access issues due to insufficient permissions. Should you require such assistance, we can provide separate professional services subject to an additional Fee.

7.3 Microsoft Sentinel Role Based Access Controls (RBAC) Permissions

Our approach to access management is based on role-based access control (RBAC) principles to ensure that individuals only have access to the information and resources necessary for their roles. The table below includes a breakdown of the roles that we require to deliver the service, and the areas each role covers. Please note that you are responsible for assigning these roles to us during Service Implementation.

Role	L1 SOC Analysts	L2 SOC Analysts	SOC Engineers
Read logs	✓	✓	✓
Create automation rules	✓	✓	✓
Create security rules	-	✓	✓
Configure settings on Sentinel	-	✓	✓
Create logic apps	-	-	✓
Read logic apps	-	✓	✓
Create support requests with Microsoft	-	✓	✓

7.4 Defender XDR RBAC Permissions

The table below includes a breakdown of the response activities that we will be able to perform across your Microsoft Defender technologies included in the scope of your Service. Please note

that our abilities to perform these response activities will depend on the technology that you have in place, the Service package that you have selected, and the access rights that you have provided to us.

The scope of the response activities listed in this Section 7.4 is dependent on the capabilities of the relevant Microsoft Defender technology on which they are performed, as offered by Microsoft, and may be subject to technical restrictions beyond our control. Please contact our SOC team if you require more information on any of these response activities.

Response activities	Endpoint	Identity	Cloud Apps	Office 365	Cloud	Comments
Isolate device	✓	-	-	-	-	
Run antivirus scans	✓	-	-	-	-	
Run baselined automated investigation	✓	-	-	-	-	
Collect investigation package	✓	-	-	-	-	
Initiate live response	✓	-	-	-	-	
Restrict app executions	✓	-	-	-	-	
Kill processes	✓	-	-	-	-	
Quarantine files	✓	-	-	✓	-	
Block or allow IPs and URLs	✓	-	-	-	-	
Modify firewall settings	✗	-	-	-	-	Firewall modifications are not included in the scope of the Service.
Remediate registry settings	✗	-	-	-	-	Registry remediations are not included in the scope of the Service.
Reset user passwords	-	✓	-	-	-	
Force user sign out	-	✓	-	-	-	
Disable or modify accounts	-	✓	-	-	-	
Adjust user risk policies	-	✓	-	-	-	
Sanction/unsanctioned apps			✓	-	-	Your prior approval is required for the performance of these actions.
Control file sharing	-	-	✓	-	-	We will report on Data Loss Prevention (DLP) based incidents, but your prior approval is required for the performance of these actions.
Governance actions	-	-	✓	-	-	
Adjust User Entity Behaviours Analytics (UEBA)	-	-	✗	-	-	
Delete or quarantine email	-	-	-	✓	-	

Anti phishing and anti-spam policies	-	-	-	✗	-	
Safe attachments policies	-	-	-	✗	-	
Enforce security recommendations	-	-	-	-	✓	We will present security recommendations, but we will not enforce them without your prior approval.
Apply adaptive application controls	-	-	-	-	✓	Your prior approval is required for the performance of these actions.
Trigger automated workflows	-	-	-	-	✓	We make automated workflows at Six Degrees, if custom ones are required, this is out of scope and will be part of a PS engagement.

✓ = Included in the Service, subject to additional comments as set out in the table

✗ = Not included in the Service

'-' = Not included in the technology

8. Service Implementation

We will agree with you the details of the implementation process and the associated key milestones based on your requirements and include details in your SoW. As a standard, the Service will be implemented based on the following delivery phases:

Mobilisation - we will commence mobilisation of resources to deliver the Service following receipt of a signed Order Form from you.

Project Kick Off - we will conduct project kick off meeting with all project stakeholders to:

(a) confirm timelines, risks, assumptions, issues and dependencies;

(b) establish stakeholder mapping, communication, and reporting frequency; and

(c) agree on elements to be included in the SoW in relation to the design phase.

Design - We will produce a Service Configuration Document aligned to what we agree with you to describe our we will operationally support your environment. The Service Configuration Document will include details of data connectors and elements included in the scope of your Service. You are responsible for approving the Service Configuration Document before we can proceed to the next implementation phase.

Implementation - We will deploy the technology to support the Service, which will include the base build and configuration of Microsoft Sentinel, including:

(a) log retention;

(b) spend caps and budget caps;

(c) user entity behaviour analytics (UEBA);

(d) health checks;

(e) review of Defender XDR policies and settings;

(f) configuration of SOC access via Azure Lighthouse and Microsoft Identity Governance; and

(g) enable bi-directional API synchronisation between Microsoft Sentinel and the SOC ticketing system.

Tuning and Optimisation - The SOC will perform tuning on your environment ahead of live service. We will work together with you through the incidents generated to reduce the number of false positives and noisy rules before going into live service. To do this, the SOC will review your environment and provide you a tuning acceptance form listing all findings and changes made to the environment rulesets. You remain responsible for signing this form.

Staging and Live Service - We will introduce you to our SOC team and prepare the implemented solution for live service.

9. Ready for Service

The Ready for Service Date is the date when we (acting reasonably and properly) notify you that the Tuning and Optimisation activities (as described in Section 8) have been completed. This date could be specified to occur at a later date, if mutually agreed to be so.

10. Billing

The Service will be billed as a Non-Recurring Fee, a Recurring Fee, and, where applicable, a Usage Fee for your Microsoft M365 licensing, Microsoft Azure, and any additional storage and usage costs that you may procure from us. Details of the applicable Fees and billing frequency will be included in your Order Form. Details of provisioning billing milestones will be listed in your Statement of Work.

We will commence billing you the Recurring Fee for the Service on or shortly after the Ready for Service Date. We reserve the right to commence billing before the Ready for Service Date if the implementation activities listed in Section 8 are delayed and such delay has arisen from: (i) your failure (or failure of your third parties) to perform your responsibilities in a timely and adequate manner; (ii) any other act or omission performed by you or your third parties; or (iii) any failure of your equipment. For the avoidance of doubt, if the completion of the implementation activities is delayed due to our acts or omissions, we will not commence billing you for Recurring Fees until the Ready for Service Date.

We will bill you the Non-Recurring Fees as set out in your SoW.

Please note that if you have procured your Microsoft licences directly from Microsoft or from a third-party Microsoft cloud service provider ("**CSP**"), you will be responsible to pay the associated charges directly to Microsoft or to the relevant CSP.

11. Termination

As a standard, we will perform the following activities before termination of your Service:

(a) Cease all connectivity to our systems.

(b) Remove your users from our systems.

(c) Cease the licensing you have procured directly from us and the access to the solution, subject to your prior approval to the removal of such licenses. If you wish to move to another CSP providers, we will keep the licenses running until you have migrated this to a new CSP. Please note that you remain responsible to pay for all charges associated with your license until they are effectively migrated to a new CSP.

(d) Remove our access from your security environments outlined in this Service Description.

(e) Remove of all our Pre-Existing IP. including rulesets, policies, automations, reports (workbooks), and hunting queries.

(f) Provide an overview to you detailing any connectivity or solution component that you should then decommission yourselves.

Please note that if you are procuring your Azure subscriptions from a CSP provider (either from us or from a third-party CSP), you will not be able to transfer such Azure subscriptions back to yourself as these can only be billed through a CSP agreement. Upon termination of the Service, we will only be able to extract your security logs and provide you with a copy of these, however the Service can be migrated to a new CSP provider.

Ahead of the service cease date, we will provide you with information on how you can maintain or download log data stored on the solution. Please note that if you wish to migrate from Microsoft Sentinel to a new provider, you may need to export the log data before termination of the Service in accordance with our guidelines.

It is your responsibility to remove any part of the solution that is hosted within your environment and to remove configurations agents and delete associated stored data. We will not be responsible for any costs incurred for solution elements that are not decommissioned, switched off or removed after termination of your Service.

Any Pre-Existing IP (as defined in the MSA) in the bespoke configuration of the Service and the Sentinel solution will remain our property and will not transfer to you or your replacement provider. Upon termination, we will remove any content that is provided under license and part of our intellectual property. This includes, but is not limited to, any part of the solution that has been developed by us as part of the baseline build of the Service, including system integrations or connectors, detection policies and automation capabilities. Any custom content that was created specifically for you will not be removed.

Please note that it is your responsibility to provide a valid termination notice in accordance with the terms of your MSA. We reserve the right to charge additional Fees for the performance of the activities listed in this Section 11 if you fail to provide a valid termination notice.

If you require us to perform any activities in addition to those listed in this Section 11, such as retention of log data, assistance with removal of any on-premise physical or virtual systems, configurations and agents, or creation of any documentation around the environment and its configuration, we can provide additional professional services subject to a separate Fee.

Any assistance that you require to hand over the solution to an alternative supplier would also be delivered as a professional service, subject to an additional Fee calculated on a time and materials basis. Please note that our intellectual property, including any rules or system configuration provided as part of the Service, will be removed from the solution before handover.

12. Exclusions

The excluded items described below are outside the scope of this Service Description:

(a) We are not responsible for any Microsoft license costs, usage costs or fees that you could incur to facilitate the delivery of this Service;

(b) We are not responsible for any update or change introduced by the SIEM solution vendor through SIEM system development or updates, including updates and changes to the graphical user interface;

(c) Tickets originating from the Service will only be sent to one of your mail group (different types of tickets cannot be sent to different mail groups and different categories, or different types of incidents cannot be sent to differing response groups). If you require different mail groups for various incident types or sources, you will need to procure additional instances of this Service. Multi-group alerting is excluded from this Service unless otherwise agreed with you in your SoW;

(d) For Microsoft Sentinel solutions, where a single SIEM instance is provisioned to ingest data from multiple subscriptions in your tenant, notifications based on a subscription level identifier are excluded and all notifications will be per tenant;

(e) For Microsoft Sentinel solutions, we you must have a Sentinel instance for every workspace where security monitoring is required by the SOC. For all multi-source solutions, where a single SIEM is provisioned to ingest data from multiple environments or domains, notifications will be based on a single client identifier;

(f) Where we have advised you that you must implement certain actions to maintain the integrity of the Service, and you fail to perform such actions within the timeframe advised by us, we will not be responsible for failures to provide the Service, and for any other loss or claim arising out of your failure to implement the required actions as notified by our SOC team; and

(g) Please note that we will have limited visibility over the changes that you may implement and the actions that you may perform in your environment. We will rely on you to keep us informed of any relevant activity or event that may impact our ability to provide the Service. Consequently, we will not be liable for failures or delays to provide the Service, and for any other loss that you may incur, where you have failed to notify us of a relevant change, action or event that may impact our ability to provide the Service.

13. Key Performance Indicators (KPI)

KPI	Calculation and measurement	Target	Measuring period	Source of measure
Standard change request completion rate	As a % of the total number of standard changes raised, the number completed within their target delivery.	95%	Monthly	IMS system
False positive rate	The number of false positives calculated as a % of the total number of SIEM alerts detected and where an incident ticket has been generated. Please note that this target is dependent upon your timely approval of tuning on your environment. We will not be responsible for failures to meet this KPI caused by your delay in the provision of the necessary tuning approval.	Within 20%	Monthly	IMS system
SIEM platform availability	The % the SIEM platform is available (excludes the availability of endpoints plus any planned outages of the SIEM platform)	100%	Monthly	Microsoft Sentinel
Mean Time To Respond (MTTR) to P1 incidents	The average time taken from the time of the incident (INC) ticket has been created to the time when the first attempt to contact your nominated contact has been made. The average time will be calculated using the Service Coverage window defined for each Priority type (specified in the *Operations Manual*).	<=60 mins	Monthly	IMS system
Mean Time To Respond (MTTR) to P2 incidents	The average time taken from the time of the incident (INC) ticket has been created to the time when the first attempt to contact your nominated contact has been made. The average time will be calculated using the Service Coverage window defined for each Priority type (specified in the *Operations Manual*).	<=2 hours	Monthly	IMS system
Mean Time To Respond (MTTR) to P3 incidents	The average time taken from the time of the incident (INC) ticket has been created to the time when the first attempt to contact your nominated contact has been made. The average time will be calculated using the Service Coverage window defined for each Priority type (specified in the *Operations Manual*).	<=4 hours	Monthly	IMS system
Average reporting frequency for P1 incidents	The average time taken by the SOC to provide you the first progress update (measured from our first attempt to contact your nominated points of contact after an incident ticket is created).	<=2 hours	Monthly	IMS system
Average reporting frequency for P2 incidents	Within the defined support coverage window for a P2, the average time the SOC provide the first progress update.	<=4 hours	Monthly	IMS system

Average reporting frequency for P3 incidents	Within the defined support coverage window for a P3, the average time the SOC provide the first progress update.	<=8 hours	Monthly	IMS system

14. Service Level Agreement

14.1 Service Credits

Service Credits shall be calculated by reference to the Recurring Fees payable in the relevant month in respect of the managed service component of the Service. For the avoidance of doubt, Usage Fees, the cost of licences and other third-party charges shall be excluded from this calculation.

The total aggregate amount of Service Credits payable in each calendar month shall not exceed an amount equal to a maximum of 10% of the Recurring Fees payable in that month in respect of the managed service component of the Service.

Ref.	Service Level	Calculation and Measurement	Target	Service Level Failure
SL01	Mean Time To Respond (MTTR)	The average time taken from the time of the IMS incident ticket has been created to the time (recorded in the IMS ticket) when the first attempt to contact your nominated contact has been made. The average time will be calculated using the Service Coverage window defined for each Priority type (specified in the *Operations Manual*).	**Incident Priority 1:** <= sixty (60) minutes **Incident Priority 2:** <= two (2) hours **Incident Priority 3:** <= 3 (three) business days	In respect of individual priority levels and for each 30 minutes above the relevant MTTR target, a credit equal to 0.25% of the Recurring Fee payable in the relevant month in respect to the manged service component of the Service, up to a maximum aggregate amount across all SLA's equal to 2.5% of such Recurring Fees.

14.2 Service Credit Exclusions

Service Credits and Service Levels are subject to the following exclusions:

(a) There are no SLAs associated with the monitoring activity carried out during the Tuning Period and the Baselining Period;

(b) There are no SLAs associated with the monitoring activity carried out during notified:

(i) periods of maintenance;

(ii) in-life tuning by the SOC;

(iii) system updates;

(c) Where you have to implement certain actions within the timeframe advised by us and your failure may have an impact on impact the integrity of the Service, we will not be responsible for failures to meet the relevant SLAs before you successfully implement the required actions as notified by our SOC team.

15. Standard Changes

You can request changes by raising a ticket on the customer portal. A change is defined as one request of the items listed in the table below.

Standard Change	Description	Measured by	Source of measurement	Target Response
Changes to the Managed Service Operations Document (MSOD)	Any changes to your information relating to contact and/or account details documented in your MSOD.	From the time the IMS request record has been raised to the time the Client has been notified the changes have been made.	IMS change request record	Within three (3) Business Days
Custom detection rule creation	Request a bespoke rule written for your environment.	From the time the IMS request record has been raised to the response time. Target delivery is the time we will take to triage the request and respond back to you with a way forward or to notify you that we have actioned the request.	IMS change request record	Within three (3) Business Days
Detection and automation policies	Enable or disable existing detection rules, playbooks or policies.	From the time the IMS request record has been raised to the response time. Target delivery is the time we will take to triage the request and respond back to you with a way forward or to notify you that we have actioned the request.	IMS change request record	Within three (3) Business Days
New detection requirement	Creation of new detection rule, playbook and policy.	From the time the IMS request record has been raised to the response time. Target delivery is the time we will take to triage the request and respond back to you with a way forward or to notify you that we have actioned the request.	IMS change request record	Within three (3) Business Days
Tuning requests	Tuning one of your specific entities or resources on incident rules. This includes changing severity, logic, and asset suppression.	From the time the IMS request record has been raised to the response time. Target delivery is the time we will take to triage the request and respond back to you with a way forward or to notify you that we have actioned the request.	IMS change request record	Within three (3) Business Days
Automation request priorities	A change to the automated response over a specific incident type.	From the time the IMS request record has been raised to the response time. Target delivery is the time we will take to triage the request and respond back to you with a way forward or to notify you that we have actioned the request.	IMS change request record	Within three (3) Business Days
Workbook Reports	Workbook reports will be provided to you directly in the Microsoft Sentinel instance. You can	From the time the IMS request record has been raised to the response time. Target delivery is the time we will take to triage the request	IMS change request record	Within seven (7) Business Days

	request up to two custom reports per month.	and respond back to you with a way forward or to notify you that we have actioned the request.		

A change is defined as one (1) request listed above.

As a standard, we offer up to four (4) standard change requests per month (included in your Service Fees). We can implement additional standard changes as and when required for an additional fee which will be defined in your Order Form or Statement of work (SoW).

Any change request that is not specifically defined in the table above will be considered a professional services engagement subject to an additional Fee calculated on a time and materials basis. These changes must follow the process covered in our MSA.