CYBER SECURITY – SERVICE DESCRIPTION

Azure Managed Sentinel

This document ("**Azure Managed Sentinel Service Description**") contains the terms governing the provision of the Azure Managed Sentinel Services provided by Interactive Pty Ltd (ABN: 17 088 952 023) of 461 Williamstown Road, Port Melbourne Vic 3207 ("Interactive") to the customer named in the CMS SOW that applies to this Service Description ("Customer").

This Azure Managed Sentinel Service Description forms part of the Agreement, also containing the Cyber Security Service Terms (found at https://www.interactive.com.au/terms-and-conditions) and the Master Services Agreement.

1 Azure Managed Sentinel Services

1.1 Interactive will provide Azure Managed Sentinel Services for the Individual Term. The Services include the ongoing monitoring, tuning and enhancement of the Customers Azure Managed Sentinel (AMS) Platform.

2 Project Delivery

2.1 Interactive will perform the following for the Project initiation:

(a) Appoint a Project Manager to:

(i) issue the Customer with Customer onboarding pack documents, which includes a customer environment discovery spreadsheet;

(ii) act as a single point of contact for all onboarding matters;

(iii) facilitate effective communication by way of updates relating to the progress of the onboarding; and

(iv) confirm an expected Project start date.

(b) Create a list of expected Monitored Event Sources as at the Service Start Date (that list is the "Monitored Event Source list").

2.2 Interactive will perform the activities set out in items 2.3, 2.4 and 2.5 as part of onboarding.

2.3 Phase 1: Providing access.

(a) Where the Customer has an existing CSP agreement with Microsoft that is managed by Interactive, Interactive will:

(i) create a CSP subscription on behalf of the Customer; and

(ii) provide delegated access to the new CSP subscription through Azure Lighthouse.

(b) Where the Customer has an existing EA, or a third party manages the Customer's CSP agreement with Microsoft, the Customer is responsible for, within 5 Business Days from the Service Start Date:

(i) creating either an EA or a CSP subscription dedicated to the Azure Managed Sentinel within the Customer's tenancy; and

(ii) providing Interactive with permission:

A. to provide delegated access to the new CSP subscription through Azure Lighthouse;

B. for Interactive to be allocated as the Digital Partner of Record ("DPOR"); and

C. to link Interactive's Partner ID to the Customer's CSP account.

2.4 Phase 2: Configuration of the Azure Managed Sentinel Platform and Related Resources (including log sources, use cases alerts, reports and Azure LogicApps Playbooks).

(a) During this phase Interactive will:

(i) Install and configure Alerts from those contained in the Interactive Detection Library that align with the onboarded log sources and complete the Incident Notification Policy that includes the details of the agreed Alert mechanism.

(ii) Install and configure a set of Azure LogicApps Playbooks;

(iii) Provide Customer support during onboarding of additional on-premises devices to the Azure Managed Sentinel Platform;

(iv) Configure custom dashboards; and

(v) Provide initial Alert tuning.

2.5 Phase 3: Initiation of management and ongoing tuning.

(a) During this phase Interactive will initiate the following activities :

(i) Management of Azure Sentinel Platform;

(ii) Tuning of security alerts & Azure LogicApps Playbooks;

(iii) Monitoring of log source availability;

(iv) Real-time alerting and integration with Customer's ticketing system;

(v) Interactive Threat Intelligence Platform feeds; and

(vi) Monthly service review meetings and optimisation reporting.

3 Acceptance Testing

3.1 On completion of the activities set out in item 2, Interactive will notify the Customer of the date the Customer may commence conducting Acceptance Tests ("Acceptance Test Commencement Date").

3.2 The Customer shall complete Acceptance Testing no later than 5 Business Days after the onboarding activities set out in item 2 are complete.

3.3 If the Customer's Acceptance Testing identifies any defects caused by Interactive that prevent the Customer from receiving the tested Services, the Customer may provide Interactive with notice in writing rejecting the Acceptance Tests and detailing the reasons why. If the Customer delivers that notice:

(a) the parties shall work together to identify and correct the error that caused the Acceptance Tests to fail; and

(b) after the cause of error is corrected, Interactive will notify the Customer of a new Acceptance Test Commencement Date and, in that event, item 3.1 will apply again.

3.4 If the Customer, acting reasonably, delivers more than two notices rejecting the results of the Acceptance Tests, either party may refer the matter for resolution in accordance with the dispute resolution provisions in the Master Services Agreement.

3.5 If the Customer fails to complete Acceptance Testing or deliver a notice rejecting the Acceptance Tests within 5 Business Days after the Acceptance Test Commencement Date, then Acceptance Testing will be deemed completed by the Customer. After all Services have completed Acceptance Testing, or are deemed to have completed Acceptance Testing, Interactive will provide the Customer with a notice informing it of the Service Start Date.

4 Subscription Tiers

4.1 The following Azure Managed Sentinel Subscription Tier Table outlines the Services that will be provided by Interactive during the Individual Term:

Azure Managed Sentinel Subscription Tier Table		
Subscription Tier	**Enhanced**	**Enterprise**
Use cases and detection ruleset	Enhanced	Enterprise
Dashboard and live reports	Delivered via portal	Delivered via portal
Alert tuning and cost optimisation	Quarterly	Monthly
Integrated threat intelligence feed	Public + Subscription	Public + Subscription
Security Orchestration and Automated Response (SOAR) Playbooks	Up to 5 changes per month	As requested via Service Requests
Azure Managed Sentinel Subscription optimisation reporting	Monthly	Monthly
Number of Service Requests	5	5

Azure Managed Sentinel Subscription Tier Table		
Inclusions:		
• Customisation of Sentinel alert rules in accordance with the Interactive Detection Library	Up to 5 changes per month	Included
• Interactive Threat Intelligence Platform feeds	Included	Included
• 3rd Party Ticketing Integration	Not included	Included
• Real-time alerting	Included	Included
• Customer support of Azure Sentinel Platform during security incidents	Included	Included
• User configuration	Included	Included
• Basic training	Included	Included
• Monitoring and reporting of license and storage consumption	Included	Included
• Manage role-based access control	Included	Included
• Manage incident notification policies (Azure LogicApps Playbooks)	Included	Included
• Monthly review of false positives	Included	Included
• Enhanced compliance reports	Optional	Included
• Tuning of security alerts & playbooks	Included	Included
• Monitoring of log source availability	Included	Included
• Customised Azure consumption reports based on specific log sources	Included	Included

*Note: Any task listed as “Optional” will be charged on a time and materials basis as set out in the Cyber Security Rate Card as published or provided.

5 Interactive Detection Library

5.1 Interactive will implement the initial detection content selected from the Interactive Detection Library in line with the entitlements of the relevant subscription.

5.2 Interactive will maintain and improve the Interactive Detection Library content in line with new threats and changes in the Customer’s IT Environment and advise the Customer that a content update is available. The Customer and Interactive will agree on the applicability of any change to Customer’s Azure Managed Sentinel Platform(s) and Interactive will implement resulting changes after impact analysis and validation. The Customer may request changes to the Interactive Detection Library content deployed to their Azure Managed Sentinel instance in accordance with the Service Request process set out in item 8. Interactive evaluates, prepares, and implements changes to the Detection Library content.

5.3 The Customer acknowledges that Interactive owns all of the Intellectual Property in the content of the Interactive Detection Library and that the content is Confidential Information. The Customer acquires no rights of ownership or title to the Confidential Information by virtue of the CMS SOW. Nothing in the CMS SOW or this Service Description limits or restricts the rights of Interactive to assert claims for infringement of intellectual property rights against the Customer. Accordingly, the parties specifically agree and acknowledge that the Customer will have no interest in the Confidential Information.

6 Threat Intelligence Platform

6.1 Interactive will provide threat intelligence enrichment on Security Events received from Monitored Event Sources to correlate Security Events with global threat and security intelligence sources. This does not require any Customer data to be sent to a third party.

6.2 Threat intelligence correlation includes detection of:

(a) blacklisted or hostile addresses targeting IT Environment;

(b) botnet communication;

(c) trojans and worms;

(d) backdoors; and

(e) open proxy attempts.

7 Data Availability and Retention

7.1 Azure Sentinel maintains Customer's logs and security incident data which Customers may access during the Individual Term. Data availability and retention will be configured in the Azure Managed Sentinel (AMS) Platform as determined by the Customer during onboarding.

8 Service Requests

8.1 The Customer may raise Simple Service Requests with Interactive to deal with common or recurring Azure Managed Sentinel and Monitored Event Source related requests, including:

(a) assisting with Customer queries and issues relating to the delivery of the Azure Managed Sentinel Platform;

(b) assisting with Customer queries and issues relating to the functionality of a Monitored Event Source where it relates to the delivery of the Azure Managed Sentinel (AMS) Platform;

(c) updating/deleting a User for various notifications;

(d) adding a User as a recipient for future reports; and

(e) tagging a Monitored Event Source as "unmanaged" in the Azure Managed Sentinel Platform whilst maintenance is being performed on the Monitored Event Source.

8.2 Interactive will provide the Customer with the number of Service Requests as included in the relevant Azure Managed Sentinel Subscription Tier set out in the Azure Managed Sentinel Subscription Tier Table. Interactive may provide additional Service Requests, as Out of Scope Work charged in accordance with the Cyber Security Rate Card.

9 Customer Responsibilities

9.1 The Customer shall:

(a) Enable and configure the Monitored Event Sources to create logs that are sent to the Managed Azure Sentinel Platform in accordance with the instructions provided by Interactive during onboarding.

(b) Enable necessary firewall rules and any other network changes to route logs to the Managed Azure Sentinel Platform.

(c) Provide an Azure dedicated management account with Contributor Access permissions required for Azure Sentinel management and configuration.

(d) Allow Interactive's technical team access to the Azure Resource Group containing the Azure Sentinel instance via Azure Lighthouse.

(e) Provide timely access to Project stakeholders to support the objectives of this Service Description.

(f) If determined to be required during Phase 1 of onboarding, provide a virtual machine or physical server for on-premises Azure Sentinel log collection. The Event Collector is required for onboarding logs from network, security devices and custom log source.

(g) If determined to be required during Phase 1 of onboarding, provide remote access to the Azure Sentinel on-premises Event Collector.

(h) Install Microsoft Monitoring Agent (MMA) software on Windows and Linux endpoints in accordance with Interactive's instructions provided during onboarding.

(i) Configure network and security devices with the details provided by Interactive in order to enable logs to be sent to the Azure Managed Sentinel Platform (i.e. syslog).

(j) Provide feedback on fine tuning of Alerts and SOAR Playbooks or LogicApps Playbooks when required.

(k) Provide detailed information on the network environment to facilitate deployment of Interactive's Azure Managed Sentinel Platform by completing the customer environment discovery spreadsheet.

(l) Ensure that its Enterprise Agreement with Microsoft is maintained during the Individual Term.

(m) Notify Interactive of any planned maintenance or outage that will impact the availability of data being ingested into Azure Managed Sentinel at least 48 hours in advance.

(n) Obtain REST API keys for SaaS Application integration.

9.2 The Customer shall not make any platform changes that may affect the availability or fidelity of Monitored Event Sources without Interactive's prior written consent. The Customer must raise a Service Request before making any changes. If the Customers fails to obtain Interactive's written consent, the Customer acknowledges and agrees that Interactive is not responsible for any Service Level failures.

9.3 If the Customer is delaying the Project, Interactive may send the Customer a notice requiring it to rectify the delay within 5 Business Days. If the Customer fails to or is unable to rectify the delay, Interactive may complete the remaining activities that are not dependent on the Customer and issue a notice confirming the Service Start Date (for the avoidance of doubt in these circumstances the provision of this notice will not require any Acceptance Tests to have occurred).

9.4 The Customer shall not use, attempt to use, or knowingly permit the use of the Services to store or transmit illegal material or in connection with any illegal, abusive or inappropriate behaviour.

9.5 The Customer must provide Interactive with a minimum of five Business Days' notice of any security testing (including but not limited to penetration testing or denial of service testing) and receive written approval from Interactive prior to proceeding. Failure to do so will result in any costs associated with responding to any Alerts caused by the testing to be charged at relevant time and materials rates identified in the Cyber Security Rate Card in addition to the suspension of any SLA targets and any associated penalties. The purpose of this item is to ensure that these activities do not impact the delivery of Services.

10 Exclusions

10.1 The following items are Out of Scope and are not included in the Services provided by Interactive unless specifically detailed in the CMS SOW:

(a) support for desktop, laptop, handheld device & smart phone;

(b) All costs related to Azure Sentinel, Azure Log Analytics and LogicApps Playbooks, fees payable to Microsoft;

(c) Configuration, troubleshooting, repair, or warranty services for cloud hosted or on-premise devices;

(d) Repair or remediation services that may be required to resolve any security, performance, or availability issues for infrastructure components owned and managed by Customer;

(e) Notifications outside of those documented in the Incident Notification Policy configured within the Azure Managed Sentinel Platform. Interactive is not responsible for a notified contact's failure to respond to the notification(s); and

(f) Unless the Customer has purchased Azure Managed Security Operations Centre (AMSOC) services under a CMS SOW, Security Event monitoring is not included in the Azure Managed Sentinel Services.

11 Deactivation

11.1 Where the Customer has an existing CSP agreement with Microsoft that is managed by Interactive, Interactive will deactivate the Azure Sentinel subscription and the Related Resources after the Individual Term is complete.

11.2 Where the Customer has an existing EA, or a third party manages the Customer's CSP subscription:

(a) Interactive will:

(i) deactivate the Related Resources after the Individual Term is complete; and

(ii) provide the Customer a written request to deactivate the Azure Sentinel subscription.

(b) The Customer must:

(i) deactivate the Azure Sentinel subscription within 14 days of receipt of the request in item 11.2(a)(ii); and

(ii) revoke all permissions provided to Interactive in accordance with item 2.3(b)(i).

12 Pricing

12.1 The Service Fees for the Services provided under this Service Description are identified in the CMS SOW and are based on the relevant Subscription Tier.

13 Limitation of Obligations

13.1 Interactive is not liable to the Customer for any delays, loss or liability suffered by the Customer where a system or the Services become unavailable due to a communication network failure, or other such causes, beyond the control of Interactive.

13.2 Interactive will not be responsible for the health, functionality or availability of data connectors released by Microsoft while they remain in 'preview mode'. Interactive may deploy these at the Customers request only and be engaged to maintain these under a separate time and materials engagement.

14 Services Levels

14.1 Interactive will provide the Service Levels in accordance with the Service Level Agreement set out at Schedule 1.

15 DEFINITIONS

Acceptance Testing means the Customer's testing of the Azure Managed Sentinel Platform to evaluate the systems compliance with the Customer's requirements specified during Onboarding.

Azure Log Analytics means a component of Azure Monitor, specifically the page in the Azure portal used to write and run queries and analyze log data. (Source: https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview)

Azure LogicApps means Microsoft Azure functionality that simplifies how you build automated scalable workflows that integrate apps and data across cloud services and on-premises systems. (Source: https://docs.microsoft.com/en-us/azure/logic-apps/)

Azure LogicApps Playbooks means the automated workflows for a Security Incident that are designed and maintained by Interactive to support Security Orchestration and Automated Response (SOAR) capability for Customer personnel.

Azure Lighthouse Azure Lighthouse enables cross- and multi-tenant management, allowing for higher automation, scalability, and enhanced governance across resources and tenants. (Source: https://docs.microsoft.com/en-us/azure/lighthouse/overview).

Azure Managed Sentinel Subscription Tier Table means the table set out in item 4.

Azure Managed Security Operations Centre (AMSOC) means the Services described in the AMSOC Service Description.

Azure Managed Sentinel (AMS) Platform means the Microsoft Azure Sentinel SIEM provided to the Customer as a managed service as a dependency of the AMSOC service.

Azure Resource Group means a container that holds related resources for an Azure solution. The resource group includes those resources that the Customer wants to manage as a group. (Source: https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-overview#resource-groups)

Azure Sentinel is a Cloud-native Security Information and Event Monitoring (SIEM) product from Microsoft Inc. (Source: https://azure.microsoft.com/en-ca/services/azure-sentinel/).

Contributor Access is an Azure role-based access control (Azure RBAC) as defined here https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles.

Complex Service Request means a request for additional Services not covered as part of a Simple Service Request.

CSP means Azure Cloud Solution Provider (source: https://azure.microsoft.com/en-au/offers/ms-azr-0145p).

EA means Enterprise Agreement with Microsoft Inc. (source: https://www.microsoft.com/en-us/licensing/licensing-programs/enterprise?activetab=enterprise-tab%3aprimaryr2).

Event Collector means a physical or virtual appliance located at the Customer location or cloud location that collects and manages logs from Monitored Event Sources to be ingested by the Azure Managed Sentinel Platform.

Incident Notification Policy is a document developed during Phase 2 of Project delivery defining how automated notifications should be sent to the Customer.

Interactive Detection Library means a Library of alerts created and maintained by Interactive for activation within the Azure Managed Sentinel Platform. Alerts developed and available in the Library are high-fidelity and specifically designed to be easily actionable by customer IT operations or security personnel.

Interactive Threat Intelligence Platform means curated threat intelligence platform developed by Interactive including a machine learning algorithm to collect, create, maintain and score threat intelligence feeds for consumption by Azure Managed Sentinel.

Microsoft Monitoring Agent (MMA) means software created and maintained by Microsoft to efficiently collect and parse log data from infrastructure.

Monitored Event Source(s) means a source of a Security Event, which may be:

(a) Service to service integration: services that are connected natively, such as AWS and Microsoft services, these services leverage the Azure foundation for out-of-the box integration, the following solutions that can be connected via service to service integration including (Azure Active Directory, Microsoft Defender for Endpoint, Office365);

(b) External solutions via API: data sources are connected using APIs that are provided by the connected data source. Typically, most security technologies provide a set of APIs through which event logs can be retrieved. The APIs connect to Azure Sentinel and gather specific data types and send them to Azure Log Analytics. Appliances connected via API include (Okta SSO, Barracuda WAF, Carbon Black Cloud);

(c) External solutions via agent: Microsoft Azure Sentinel can be connected via an agent to any other data source that can perform real-time log streaming using the Syslog/CEF protocol. External solutions connected via agent include (Palo Alto Network firewalls, Zscaler proxy, Fortinet firewalls);

(d) a single host source (such as a workstation, PC, laptop, desktop, mobile, tablet or desktop AV agent);

(e) a server source (such as an application, database, web services, authentication services or server operating system); or

(f) a Network source (such as a firewall, Network IPS, mail/web security gateway, proxy, DDoS mitigation or load balancer).

Partner ID means the ID used to associate the Customer accounts with Interactive's account.

Project means all work to be performed during onboarding and Acceptance Testing to deliver the Services to the Customer in accordance with this Service Description.

Project Manager means the Interactive or Customer staff member responsible for delivery of the Services set out in this Service Description.

Related Resources means the subscription created for Azure Sentinel, resources, detections deployed by Interactive, and Azure LogicApps Playbooks and Azure Workbooks (which are each functions of Azure Sentinel).

Security Event means a condition or situation detected by the Azure Managed Sentinel Platform, which is observed from one or more Monitored Event Sources.

Service Start Date means the earlier of the date notified by Interactive in accordance with item 3.5 or item 9.3 for all Services, or the date the Customer accepts the results of Acceptance Testing for all Services.

Service Request for the purposes of the Service Level Agreement means a request for service from the Customer, which may be a Simple Service Request or Complex Service Request, that is a move, add, change or delete to the Azure Managed Sentinel Services (excluding Incidents).

Subscription Tier means the level of Azure Managed Sentinel service, which may be Enhanced or Enterprise as set out in the Azure Managed Sentinel Subscription Tier Table.

User means a named user of the Customer's Microsoft Active Directory (or other similar application) and Users means each one of them.

Schedule 1 Azure Managed Sentinel Services Service Level Agreement (SLA)

1 Service Level Agreement

1.1 Interactive will endeavour to meet the Service Levels, however the Customer acknowledges that a Failure is not deemed to be a breach of the CMS SOW as it relates to the Azure Managed Sentinel Services.

2 Incident Reporting Procedure

2.1 If a Customer experiences an Incident, the Customer must take all reasonable steps to ensure that the Incident is not a fault within the Customer's Responsibility Domain before reporting the Incident to Interactive.

2.2 If the Customer is satisfied that the Incident is not due to an issue within its Responsibility Domain, the Customer may report the Incident to Interactive's Service Desk as follows:

Phone: 1300 669 670 (in Australia) or +61 2 9200 2679 (internationally)

Online: http://www.interactive.com.au/support

Email: support@interactive.com.au

2.3 When reporting an Incident, Customers must provide the following information to Interactive:

(a) Customer Name and service(s) affected by the Incident.

(b) Description of the Incident, including the Customer's classification of the urgency and impact of the Incident in accordance with Table 1 and Table 2.

(c) Name and contact details of the person reporting the Incident.

(d) Name and location of the site affected by the Incident.

(e) Business / trading hours of the site affected by the Incident.

2.4 The Service Desk provides a 24 x 7 x 365 service for severity 1 and 2 Incidents and Business Hours for other Incidents and Service Requests.

2.5 Severity 1 and Severity 2 Incidents must be logged by telephone only. Severity 1 and Severity 2 Incidents not logged by telephone are exempt from the calculation of Service Levels. Severity 3 and Severity 4 Incidents may be logged by telephone or email.

2.6 Interactive, at its sole discretion, may charge the Customer a reasonable amount, based on the Standard Charge Out Rate, to diagnose an Incident if the Customer knew, ought to have known, or would have known following reasonable investigation, that the Incident was not caused by Interactive, or was caused by something within the Customer's Responsibility Domain.

3 Initial Impact Assessment

3.1 Interactive will determine the severity of any reported Incident based upon the Customer's impact assessment having regard to the urgency and impact definitions in Table 1 and Table 2. Interactive will then allocate a severity level in accordance with Table 3.

3.2 Where there is doubt regarding impact to a significant number of users or a few users, Interactive will be conservative and classify the Incident at the next highest level. Incident or problem severity level classification may be changed later with a valid reassessment.

3.3 If the Customer disagrees with Interactive's classification of an Incident, the Customer may escalate the matter to Interactive's Contract Representative to discuss the classification, rather than Interactive assigning a higher severity.

Table 1 Urgency Definitions

URGENCY			
Critical	**High**	**Medium**	**Low**
Critical business function impacted.	Important business function is impacted.	Administration activities impacted.	Business function continues.

Table 2 Impact Definitions

IMPACT			
Critical	**High**	**Medium**	**Low**
All Customer users are affected.	All business unit or department users are affected.	All team users are affected.	Only an individual is affected.

Table 3 Severity Definitions

SEVERITY		**IMPACT**			
		Critical	**High**	**Medium**	**Low**
URGENCY	**Critical**	SEV 1	SEV 2	SEV 2	SEV 3
	High	SEV 1	SEV 2	SEV 3	SEV 4
	Medium	n/a	SEV 3	SEV 4	SEV 4
	Low	n/a	SEV 4	SEV 4	SEV 4

4 Response and Update Service Levels

4.1 The response and update times are calculated starting from when the Customer first notifies Interactive about the Incident in accordance with item 2.3.

4.2 Interactive is deemed to have met each of the Service Levels as follows:

(a) For the Response Time Service Level (set out in Table 4):

(i) In respect of Severity 1 and 2 Incidents – the time calculated from the time the caller provides all mandatory details until the time the caller is provided with an Incident ticket number; or

(ii) In respect of Severity 3 and 4 Incidents or Service Requests - the time calculated from the time an email is received or telephone call is made providing all mandatory details until the initiator is emailed an Incident/Service Request ticket number in return.

(b) For the Update Time Service Level (set out in Table 5): by providing updates to the Customer about the Incident by phone or email.

(c) For the Restoration Service Level (set out in Table 6): by Restoring the Incident.

(d) For the Service Request Service Level (set out in Table 7): by actioning the Service Request.

Table 4 Response Time Service Level

Severity Level	Classification Description	Response Time - Incidents logged by Telephone or Email (Business Hours for Severity 3-4)	
		Enhanced	Enterprise
Severity 1	Critical	< 1 hour	< 30 mins
Severity 2	High	< 2 hours	< 1 hour
Severity 3	Medium	< 2 Business Days	< 1 Business Day
Severity 4	Low	< 2 Business Days	< up to 1 Business Day
Severity 20	Service Request	< 2 Business Days	< up to 1 Business Day

Table 5 Update Time Service Level

Severity Level	Classification Description	Update Time - Incidents logged by Telephone or Email (Business Hours for Severity 3-4)	
		Enhanced	Enterprise
Severity 1	Critical	2 hours	1 hour
Severity 2	High	4 hours	2 hours
Severity 3	Medium	< 2 Business Days	< 1 Business Day
Severity 4	Low	< 2 Business Days	< 1 Business Day

5 Restoration Targets

5.1 The Restoration Service Levels are set out in Table 6. Interactive will endeavour to Restore the Azure Managed Sentinel Services after an Incident, to the extent the Incident is within Interactive's Responsibility Domain.

Table 6 Restoration Service Levels

Incident Priority Classification	Classification Description	Restoration Time (Business Hours for Severity 3-4)	
		Enhanced	**Enterprise**
Severity 1	Critical	< 1 Business Day	< 4 hours
Severity 2	High	< 2 Business Days	< 8 hours
Severity 3	Medium	4 Business Days	2 Business Days
Severity 4	Low	4 Business Days	4 Business Days

6 Service Request Targets

6.1 Interactive will endeavour to resolve a Simple Service Request, or Priority Service Request, within the Target Completion Time set out in Table 7. The Target Completion Time begins from when the Service Request is logged by the Customer, or the Account Executive or Service Delivery Manager on the Customer's behalf.

6.2 A **Simple Service Request** is a request from the Customer for a simple move, add, change or delete to Azure Managed Sentinel Services, determined by the Interactive to be a request that:

(a) is non-complex and does not require planning or due diligence;

(b) can be completed in 4 hours or less, by a single engineer and during Business Hours; and

(c) does not require representation at Interactive's change advisory board.

6.3 If the Customer makes a request that is not a Simple Service Request, or requires planning, due diligence, multiple engineers, dedicated infrastructure or will take multiple days to complete, Interactive will treat these requests as a standalone project ("**Complex Service Request**"). Interactive will provide estimated delivery timelines for complex requests as part of the project plan, which is developed in consultation with the Customer during the project and is not subject to the Service Levels set out in Table 7. Interactive cannot guarantee project delivery timelines for requests that are not Simple Service Requests, as timelines vary depending infrastructure availability from suppliers and each party's resource availability.

Table 7 Service Request Service Levels

Incident Priority Classification	Classification Description	Target Completion Time	
		Enhanced	**Enterprise**
Severity 20	Simple Service Request	5 Business Days	4 Business Days
	Priority Service Request	2 Business Days	2 Business Days

7 Excused Disruptions

7.1 Interactive is not liable for any Failures caused or contributed to by:

(a) underlying infrastructure managed by a CRP, including Cloud Resources;

(b) the Customer, its contractors or representatives;

(c) a Force Majeure event;

(d) any Planned Outage Period;

(e) communication links, including those provided by Interactive; or

(f) any Third Party Fault.

8 Definitions

Cloud Resources means the CRP's online services the Customer subscribes to directly with the CRP.

CRP means:

(a) for Microsoft Azure Cloud Resources, the CRP is Microsoft Corporation; and

(b) for Amazon AWS Cloud Resources, the CRP is Amazon Web Services, Inc.

CRP Terms means the Microsoft Terms, the AWS Terms, and any third party terms (such as a EULA) that apply to provisioned licenses between the Customer and the CRP, and **CRP Term** means either one of them.

Digital Partner of Record ("DPOR") means an on-line capability to attach a specific partner to a customer's Microsoft on-line subscription.

Failure means where Interactive fails to achieve a Service Level in any given month, other than where it is attributed to any excused event referred to in the SLA.

Incident means an unplanned interruption to the standard operation of Azure Managed Sentinel Services that disrupts the quality of the Azure Managed Sentinel Service.

Microsoft Terms means the Microsoft Online Subscription Agreement, Online Service Terms, Microsoft Cloud Agreement, and the Microsoft Service Levels, which are available online at the Microsoft website, or on request from Interactive, and any other terms or policies referred to in those Microsoft terms or that apply to the Azure Managed Sentinel SIEM services. Microsoft Terms includes the following:

- Cloud Agreement: https://docs.microsoft.com/en-us/partner-center/agreements
- Online Services Terms: https://www.microsoftvolumelicensing.com/Downloader.aspx?documenttype=OST&lang=English
- Online Subscription Agreement: https://azure.microsoft.com/en-au/support/legal/subscription-agreement
- Service Levels: https://azure.microsoft.com/en-au/support/legal/sla

Planned Outage Period means an outage period declared by Interactive or a CRP for any reason, including maintenance requirements on a facility, networks, infrastructure or systems, de-installation of infrastructure, or infrastructure, firmware or software currency upgrades.

Priority Service Request means a Simple Service Request that has been upgraded in accordance with the process set out in the security operations manual created in accordance with the AMSOC Service Description.

Responsibility Domain means, in relation to a party, equipment or networks owned or managed by the party, or anything provided by a third party engaged by the party.

Restoration means, in relation to a Managed Service, the return to correct operability, which may be achieved by temporary measures, and **Restored** has a corresponding meaning.

Service Desk means the first point of contact between Interactive and the Customer in respect of reporting and communicating Incidents.

Service Level means one of the service levels described in the SLA.

Third Party Fault means an Incident affecting Azure Managed Sentinel SIEM where:

(a) the root cause is solely or partly the responsibility of a third party, such as a telecommunications provider;

(b) the Incident is wholly or partly dependent on a third party for Restoration;

(c) the Incident is caused by an issue with hardware, networks or software and the vendor or manufacturer of the hardware, network or software has not issued a patch or other fix to remedy the Incident; or

(d) the Incident is caused by a new or undocumented issue that is inherent in the Services.