CYBER SECURITY – SERVICE DESCRIPTION

Azure Managed Security Operations Centre Services

This document ("AMSOC Service Description") contains the terms governing the provision of the Azure Managed Security Operations Centre 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 AMSOC Service Description ("Customer").

This AMSOC 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 Security Operations Services

1.1 Interactive will provide AMSOC Services for the Individual Term. The AMSOC provides the Customer with a detection and response capability for an Azure Managed Sentinel Service (and the Azure Managed Sentinel Service is detailed in a separate Service Description).

1.2 The Service Start Date for the AMSOC Services is one of the following, as applicable:

(a) If the Customer has purchased AMSOC concurrently with Azure Managed Sentinel, on the later of: (i) the date that Acceptance Testing is completed or deemed completed under the Azure Managed Sentinel Service Description; and (ii) the completion of the activities identified in item 2.1; or

(b) If item 1.2(a) does not apply (because the Customer has purchased AMSOC at another time), the date notified by Interactive to the Customer in accordance with item 3.

1.3 From the Service Start Date Interactive will:

(a) commence Monitoring activities as set out in item 9; and

(b) commence Security Incident Management activities as set out in item 10.

2 Onboarding

2.1 Interactive and the Customer will work together to:

(a) develop a security operations manual; and

(b) confirm categorisation of critical Monitored Event Sources.

2.2 If item 1.2(b) applies, Interactive will perform the following additional onboarding process to enable initiation of management and ongoing tuning:

(a) Interactive will:

(i) initiate integration with Interactive's SOAR platform;

(ii) undertake a baseline review of security alerts; and

(iii) review and update tuning of security alerts,

2.3 Prior to the Service Start Date, but after completion of the activities in item 2.1 and (where applicable) Acceptance Testing conducted in accordance with item 3, Interactive will:

(a) send the Customer a welcome notification containing the procedure for contacting the Service Desk; and

(b) provide the Customer with the security operations manual.

3 Acceptance Testing

The following is applicable if item 1.2(b) applies:

3.1 On completion of the activities set out in item 2.1(b) 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 0 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 AMSOC Subscription Tier Table outlines the AMSOC Services that will be provided by Interactive during the Individual Term:

AMSOC Subscription Tier Table		
Subscription Tier	**Enhanced**	**Enterprise**
Security Event Triage and Notification	Included	Included
Security Incident Investigation and Escalation (S1, S2)	24 x 7	24 x 7
Security Incident Active Response	Not Included. Can be provided if the Customer purchases an MDR Service; or an Incident Response Service.	Not Included. Can be provided if the Customer purchases an MDR Service; or an Incident Response Service.
Crisis Management	Not included	Included
Advanced Threat Detection capability:		
• Advanced logging methodology aligned to risk-based detections	Included	Included
• Attack Simulations (Purple Team Exercises)	Yearly	Quarterly
• Detection Maturity – Threat Coverage Heatmap mapped to MITRE ATT&CK	Included	Included
Advanced Threat Detection capability:		
• Data Quality Maturity – Threat Coverage Heatmap mapped to MITRE ATT&CK	Not included	Included
Service Delivery:		
• SLA's	Included	Included
• Ticketing system integration	Included	Included
• Service reporting and review (11.4 Cyber Security Operations workshop)	Optional	Monthly
• Risk reporting and tracking for critical assets (NIST risk chart) (11.5 Cyber Risk Strategy workshop)	Bi-annually	Quarterly
• Service Request	5 Service Requests	5 Service Requests
• Board & Executive calls	Optional	Bi-annually

*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 Monitored Event Sources

5.1 The Customer must ensure the Monitored Event Sources are and remain in a Healthy, Functional and Tuned Operational State, where:

(a) "**Healthy**" means there are no known hardware/software issues or bugs affecting the operation or management of the Monitored Event Source;

(b) "**Functional**" means the Monitored Event Source has been specified and designed correctly, configured and operationally effective (as determined by Interactive); and

(c) "**Tuned**" means the Monitored Event Source has been configured according to the needs and relevance of the Customer's IT Environment, which includes minimising false positive alerts and ensuring redundant or unnecessary configurations are removed.

5.2 Interactive will tune the Monitored Event Source based on information provided by the Customer during onboarding.

5.3 The Customer must configure the Monitored Event Sources to send events or logs to the Event Collector and perform regular reviews of alerts and signatures to ensure appropriate levels of logs are being delivered to the Event Collector.

5.4 Interactive may terminate data/log collection from a Monitored Event Source which is not in an Operational State.

5.5 If the IT Environment or any part of it (including any Monitored Event Source) is found to require changes to be in an Operational State, the Customer must:

(a) request Interactive to perform any necessary work as Out of Scope Work;

(b) perform any necessary changes itself, or via a third-party provider; or

(c) elect to exclude a Monitored Event Source that is not in an Operational State from the AMSOC.

5.6 It is the Customer's responsibility to ensure that the Monitored Event Source list is up to date. The Customer must make a Service Request to request to add or delete Monitored Event Sources from the Monitored Event Source List.

5.7 To allow Interactive to provide the AMSOC, the Customer may be required to make modifications to some Monitored Event Sources, as advised by Interactive. This may include making changes to firewalls and/or access control lists (sometimes referred to as ACLs) that block Interactive management traffic on the Network. Interactive can assist with changes to a Monitored Event Source on request as Out of Scope Work.

5.8 Where there are two or more physical devices (for example, firewalls) configured in an active/passive state sharing a common single floating IP between the physical devices, the devices are deemed a single Monitored Event Source. Where multiple end points (hosts) send Security Events to a central management console, each end point is deemed a single Monitored Event Source.

5.9 A device may be a Monitored Event Source if it can be found on the Supported Data Sources List. If the Customer requires a device to be a Monitored Event Source that is not found on the Supported Data Sources List, the Customer must request Interactive provision custom parsers for those devices as Out of Scope Work.

6 Threat Coverage Heatmap

6.1 From the Service Start Date, if the AMSOC Subscription Tier Table states that Threat Coverage Heatmap forms part of the offering of the Subscription Tier that the Customer has acquired, Interactive will provide a report (known as the "Threat Heatmap Report") represented as a MITRE ATT&CK Heatmap to display current threat detection coverage based on:

(a) Detection rules currently deployed via the Azure Managed Sentinel Service in accordance with the Azure Managed Sentinel Service Description; and

(b) Quality of data being ingested into the Azure Managed Sentinel platform from Monitored Event Sources.

6.2 The frequency of any subsequent Threat Heatmap Report is stipulated in the AMSOC Subscription Tier Table.

7 Attack Simulations

7.1 After deploying the Interactive Detection Library and as stipulated in the AMSOC Subscription Tier Table, Interactive will perform non-destructive attack simulations to validate detection capability and compliance of logging methodology deployment against Monitored Event Sources.

7.2 Post attack simulation activity, Interactive will perform a review to determine the effectiveness of current threat detection capability and will provide a report (known as the “Attack Simulation Report”).

7.3 The frequency of any subsequent Attack Simulation Report is stipulated in the AMSOC Subscription Tier Table.

7.4 The Customer must provide Interactive with a minimum of 5 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 in accordance with the security operations manual provided in accordance with item 2.3(b). Failure to do so will result in any costs associated with responding to any alerts caused by the testing to be charged at the time and materials rates set out in the Cyber Security Rate Card in addition to the suspension of any Service Levels and any associated penalties. The purpose of this provision is to ensure that these activities do not impact the delivery of Services.

8 Changes to Monitored Event Sources and Event Collector

8.1 The Customer must:

(a) not make any changes to the IT Environment that will adversely affect the operation of one or more Monitored Event Sources, Event Collectors or Azure Resource Group;

(b) notify Interactive (by way of a Service Request) of all changes made, or to be made, by the Customer (or third party on behalf of the Customer), to:

(i) one or more Monitored Event Sources, Event Collectors or Azure Tenancy; or

(ii) the IT Environment or configuration of the Customer’s data or telecommunication networks that affect, or may affect, a Monitored Event Source and/or Event Collectors; and

(c) Notwithstanding items 5.5 and 8.1(a), if the Customer makes any changes without complying with item 8.1(b) (such changes are “Unauthorised Changes”), the Customer must rectify the Unauthorised Change (or engage Interactive to do so as Out of Scope Work) to ensure the Monitored Event Sources and/or Event Collectors are in an Operational State.

8.2 Interactive is not 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 Customer’s request only and be engaged to maintain these under a separate time and materials engagement. Security Incidents that are created as a result of a Support Data Source that is in ‘preview mode” are not subject to the SLA’s in this Service Schedule.

8.3 Where the Customer manages Monitored Event Sources that Interactive is providing AMSOC services for, the Customer must provide a qualified resource to perform tuning action as requested by Interactive. Tuning of the following items will be performed in the order requested by Interactive:

(a) Azure Security Center;

(b) Defender for Endpoint;

(c) Defender for Identity;

(d) Defender for 365;

(e) Microsoft Cloud Application Security and Azure Defender (to be performed by the Customer);

(f) Sentinel (to be performed by Interactive); and

(g) Security orchestration and automated response (SOAR) (to be performed by Interactive).

8.4 If the Customer does not perform tuning on the requested platforms within 10 Business Days, Interactive may charge the Customer time and materials rates as set out in the Cyber Security Rate Card to triage any related alerts.

8.5 Interactive will charge the Customer for AMSOC provided in response to Security Incidents caused by Unauthorised Changes made to a Monitored Event Source, Event Collector or Related Resources. Additional charges will be based on the number of hours required to remediate an unapproved change and charged at the Standard Charge Out Rate.

9 Monitoring

9.1 Interactive will monitor the Monitored Event Sources via the Azure Managed Sentinel Platform to detect and capture Security Events during the timeframes determined in the relevant Subscription Tier.

9.2 Interactive will provide outcomes-based monitoring and analysis to predict Security Incidents based on a suspicious series of Security Events, which is intended to provide the Customer with an early warning system of possible future threats.

9.3 Interactive will include notifications obtained through monitoring as part of the Security Incident Management Process.

9.4 Interactive will integrate the Azure Managed Sentinel environment with Interactive's cloud based security orchestration and automated response (SOAR) platform to provide enrichment of incident data.

9.5 From the Service Start Date, Interactive will perform security alert baselining for a period of 4 weeks. During this period, the Service Levels will not apply to alert management.

10 Security Incident Management

10.1 Interactive will perform the Security Incident Management Process for each Security Incident. The phases of the Security Incident Management Process are:

(a) Phase 1: Security Incident Identification;

(b) Phase 2: Security Incident Investigation;

(c) Phase 3: Security Incident Response and Containment;

(d) Phase 4: Security Incident Rectification;

(e) Phase 5: Restart; and

(f) Phase 6: Monitoring.

10.2 Interactive will provide the Customer with up to 1 hour of support for each phase of the Security Incident Management Process. Any additional time spent will be charged at the Standard Charge Out Rate.

10.3 **Phase 1: Security Incident Identification**

(a) After a Security Incident is detected by Interactive or reported to Interactive by the Customer, Interactive will perform the following:

(i) Identify the source and impacted resources associated with the Security Incident.

(ii) Confirm the Security Incident has been generated from an analytics rule as part of Interactive Detection Library. If the Security Incident generated is determined to be a false positive, Interactive will close the ticket and tune the system in accordance with the security operation manual referred to in item 2.3(b) in order to avoid recurrence.

(iii) Establish the severity level of the Security Incident in accordance with Table 1.

(iv) For Security Incidents categorised as Severity Level 3 or 4:

A. notify the Customer of Security Incidents according to the protocol set out in the Customer's operations manual (which may be by ticket, email, telephone or as a daily/weekly/monthly digest);and

B. close the incident and store the information for historical reporting purposes.

(v) For Security Incidents categorised as Severity Level 1 or 2:

A. treat these as critical Security Incidents (to be treated as per operations manual) and raise an incident record;

B. conduct an initial diagnosis by a security analyst as to the cause of Security Incidents; and

C. notify the Customer of Security Incidents according to protocol set out in the Customer's operations manual (which may be by ticket, email or telephone).

(b) Interactive will endeavour to respond to Security Incidents in accordance with the Response Time Targets set out in Table 2.

Table 1.	**Severity Levels**
1. Critical	• Successful penetration or denial of service Attacks detected with significant impact on the organisation with one or more of the following elements: – very successful, difficult to control or counteract; – large number of systems compromised; – significant loss of confidential data; and/or – loss of critical systems or applications. • Significant risk of negative financial or public relations impact. • Significant systems degradation/loss due to a virus or worm outbreak that cannot be handled by installed anti-virus software or security controls. • A verified widespread Attack.

Table 1.	Severity Levels
2. High	• Penetration or denial of service Attack(s) detected with limited impact on the organisation, with one or more of the following elements: – minimally successful, easy to control or counteract; – small number of systems compromised; – little or no loss of confidential data; and/or – no loss of critical systems or application. • Widespread instances of a known computer virus or worm that cannot be handled by deployed anti-virus software or security controls with one or more of the following elements: – small risk of negative financial or public relations impact; and/or – a verified Attack but limited to certain assets.
3. Medium	• Significant level of Network probes, scans, and similar activities detected indicating a pattern of concentrated reconnaissance. • Penetration or denial of service Attack(s) attempted with no impact to the Customer. • Widespread instances of a known computer virus or worm, easily handled by deployed anti-virus software or security controls. • Isolated instance of a new computer virus or worm that cannot be handled by deployed anti-virus software.
4. Low	• Small numbers of system probes, scans and similar activities detected on the Customer's internal systems. • Intelligence received concerning threats to which the organisation may be vulnerable.

Table 2.	Response Time Targets
Severity Level	Response Time
S1	0.5 hours
S2	1.5 hours
S3	4 hours
S4	8 hours

10.4 **Phase 2: Security Incident Investigation**

(a) After the Security Incident Identification phase, Interactive will provide remote support to:

(i) assist the Customer to determine the source of events that lead to the Security Incident being generated. Recommendations will be provided to assist the Customer to contain and/or eradicate the threat, using the information obtained and enriched through the investigation process.

(ii) assist the Customer to decide on a state of lockdown, including whether to:

A. monitor and record the Threat Actor's actions if the Threat Actor has compromised isolated or minor systems where the Security Incident is an Attack;

B. shut down or isolate the Network component or segment if the Threat Actor has compromised administrative privilege across many machines; or

C. pursue another course of action as per the Customer's operations manual;

(iii) assist the Customer to identify the means through which the Threat Actor gained access using the available data already collected by the Event Collector; and

(iv) copy and safely store audit trails, log files and intrusion traces from any Monitored Event Sources that were targeted and provide these via secure communication channel and Interactive will securely delete the data referred to in this item on termination of the CMS SOW unless requested prior by the Customer.

(b) The Customer must use reasonable endeavours to do the following as and when required by Interactive:

(i) provide a qualified point of contact to assist with Interactive's investigation of the Security Incident;

(ii) verify that all logs and logging systems for other devices have not been tampered with by the Threat Actor;

(iii) conduct a rapid survey of the Network and list of devices and systems that may be contaminated;

(iv) take reasonable actions to obtain information pertaining to the Security Incident in a reasonable timeframe;

(v) copy and safely store audit trails, log files and intrusion traces from any other devices that were targeted; and

(vi) notify Interactive about any changes that may impact on the AMSOC and when the Security Incident has been resolved.

10.5 **Phase 3: Security Incident Response and Containment**

(a) After the Security Incident Investigation phase, Interactive will provide remote support in one of the following ways:

(i) If the Monitored Event Source is provided by Interactive to the Customer under a separate agreement for the provision of cloud IaaS services, Interactive will:

A. inform the Interactive teams of the Security Incident; and

B. work with the Interactive teams to perform the Customer requirements set out in item 10.5(b).

(ii) If the CMS SOW states the Customer receives MDR Services and Interactive has been provided Authority to Act, Interactive will perform all containment and eradication activities that are available through the MDR Cloud Platform for the MDR Services.

(iii) If a supported Endpoint Detection and Response tool has been integrated with the SOAR Playbooks capability and a Monitored Event Source is actively compromised through malware:

A. Interactive will respond by quarantining the device, such that the Monitored Event Source may only communicate with the Endpoint Detection and Response platform and stop running any non-essential processes and services;

B. Interactive may quarantine the Monitored Event Source before notifying the Customer to stop a threat before propagating to the wider Network; and

C. Interactive may remove malicious software identified on Assets or hosted on the Network (via shared drives/folders) in consultation with the Customer.

(iv) If neither item 10.5(a)(i) or (ii) applies, the Customer may request Interactive perform active response measures (such as those set out in items 10.5(a)(i) or (ii)) as Out of Scope Work. The Customer acknowledges and agrees that Interactive does not guarantee resources will be available to provide active response measures at the time of a Security Incident.

(b) The Customer must use reasonable endeavours to do the following as and when required by Interactive:

(i) make contact with the end user related to the Security Incident to gather further detail, to confirm or disprove malicious activity.

(ii) if the Customer implements a lockdown or quarantine of any part of the IT Environment, verify that parts of the IT Environment required to apply the lockdown are stable and trustworthy;

(iii) deny all access to the Network by the Threat Actor and log all subsequent attempts at communication from the Threat Actor for later analysis;

(iv) close the apparent means of entry, which may be temporary (such as denying all inbound traffic to a particular service) or permanent (such as repairing the hole); and

(v) notify Interactive about any changes that may impact on the AMSOC and when the Security Incident has been resolved.

10.6 **Phase 4: Security Incident Rectification**

(a) After the Security Incident Response and Containment phase, Interactive will provide remote support to:

(i) assist the Customer to confirm (and, if Interactive considers appropriate, duplicate) the Threat Actor's means of entry and analyse the Threat Actor's modifications to determine any secondary means of entry;

(ii) if possible, review whether the Monitored Event Source is in an Operational State; and

(iii) provide advice and/or assistance to the Customer on restoring a contaminated Monitored Event Source to an Operational State. Any advice or assistance provided will be deemed Out of Scope Work.

(b) The Customer must use reasonable endeavours to do the following as and when required by Interactive:

(i) verify the integrity of its Network components;

(ii) apply any additional lockdown that may be required;

(iii) rebuild any contaminated Network components;

(iv) close or develop a workaround for the Threat Actor's means of entry; and

(v) notify Interactive about any changes that may impact on the AMSOC and when the Security Incident has been resolved.

10.7 **Phase 5: Restart**

(a) After the Security Incident Rectification phase, Interactive will provide remote support to:

(i) confirm with the Customer that all Network systems or services are working properly;

(ii) make recommendations as to the appropriate third party notifications to be made; and

(iii) provide the Customer with the information that was collected during the previous phases so that the Customer can take other action as the Customer considers appropriate.

(b) If a Threat Actor block has been put in place to contain an Attack or potential Attack, the Customer must leave the Threat Actor block in place for the period required by Interactive, unless the parties agree otherwise.

10.8 **Phase 6: Monitoring**

(a) After the Restart phase, Interactive will monitor for subsequent related activity from the Customer's IT Environment or the Threat Actor's means of entry, until Interactive deems the threat to be removed or mitigated.

11 Reporting

11.1 One month after the Service Start Date on an ongoing monthly basis, Interactive will provide a report (known as the "Cyber Security Report") to the Customer, which contains the following information:

(a) Threat Heatmap Report, where applicable to the Subscription Tier;

(b) Attack Simulation Report, where applicable to the Subscription Tier;

(c) updated Monitored Event Source List;

(d) asset inventory trend;

(e) Security Incidents where applicable;

(f) top targeted hosts;

(g) top 10 successful authentications; and

(h) top 10 failed authentications.

11.2 Interactive will present the Cyber Security Report to the Customer during a monthly meeting.

11.3 Additional customised reports are available on request from the Customer, which will be treated as Out of Scope Work.

11.4 Cyber Security Operations workshop: During Business Hours, at the frequency specified in the AMSOC Subscription Tier Table relevant to the Subscription Tier acquired by the Customer, Interactive will facilitate a meeting between the Customer and an Interactive analyst to:

(a) discuss strategic quarterly findings;

(b) discuss trends of Attacks;

(c) discuss operational SLA metrics;

(d) discuss the Customer security roadmap and changes to the IT Environment; and

(e) make recommendations about the Customer's security posture.

11.5 Cyber Risk Strategy workshop: During Business Hours, at the frequency specified in the AMSOC Subscription Tier Table relevant to the Subscription Tier acquired by the Customer, Interactive will facilitate a meeting between the Customer and an Interactive Cyber Risk and Governance consultant to discuss:

(a) any updates to the Customer's business and potential impact on risk profile;

(b) key improvements to security program and risk reduction;

(c) effectiveness of AMSOC to reduce cyber risk; and/or

(d) priority activity for the next quarter.

12 Service Desk

12.1 Interactive will provide a Service Desk function that:

(a) acts as the service interface for all aspects of the AMSOC;

(b) is available to the Customer to raise Security Incidents and Service Requests by telephone or email 24 hours per day, 365 days a year;

(c) creates and maintains records of Security Incidents and Service Requests in the Interactive management system and provides the Customer with a reference number for assistance in subsequent interaction with the Service Desk;

(d) if the Customer submits a Security Incident or Service Request by email, sends a confirmation email containing the reference number;

(e) provides regular updates to the Customer on the progress of Security Incidents and Service Requests and ensure that they are completed prior to closing them in the Interactive management system; and

(f) processes Security Incidents and Service Requests assigned to the Monitored Event Source.

12.2 The Customer must:

(a) ensure that Security Incidents and Service Requests are only raised with the Service Desk by authorised personnel as determined in the security operations manual referred to in 2.3(b) and as notified to Interactive. Such authorised personnel must have a good understanding of the AMSOC;

(b) follow the Service Desk logging procedures and provide sufficient and accurate information for the Service Desk to respond to the Security Incidents or Service Requests without delay;

(c) raise Severity 1 and 2 Security Incidents with the Service Desk by telephone;

(d) if requested by Interactive, perform an initial diagnosis on a Security Incident; and

(e) escalate Security Incidents to Interactive only if they cannot be resolved internally.

13 Service Requests

13.1 The Customer may raise Service Requests with Interactive to deal with common or recurring AMSOC and Monitored Event Source related requests, including:

(a) assisting with Customer queries and issues relating to the delivery of the AMSOC;

(b) assisting with Customer queries and issues relating to the functionality of a Monitored Event Source where it relates to the delivery of the AMSOC;

(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 Interactive SIEM whilst maintenance is being performed on the Monitored Event Source.

13.2 Interactive will provide the Customer with up to five Simple Service Requests per month. Interactive may provide additional Simple Service Requests, or Service Requests that are not Simple Service Requests, as Out of Scope Work charged in accordance with the Cyber Security Rate Card.

14 Service Exclusions

14.1 The Customer agrees and acknowledges Interactive is not required to contain or eradicate any threats, vulnerabilities or Attacks, except as set out in item 10.5(a). Interactive is not liable for any loss or liability incurred by the Customer in connection with a threat, vulnerability or Attack not being detected, contained or prevented unless Interactive was required by items 10.5(a)(ii) and 10.5(a)(iii) to do so and it was not detected or prevented directly due to Interactive's gross negligence or intentional misconduct.

14.2 Interactive does not, and cannot, warrant that it will detect or prevent all threats, incidents or vulnerabilities to the Monitored Event Sources.

14.3 The AMSOC does not include any of the following:

(a) Anything not included in this AMSOC Service Description as being part of the AMSOC.

(b) Configuration of security systems and devices to allow for log collection by Event Collectors.

(c) Configuration of the VPN end tunnel on the Customer Location.

(d) Security device application management.

(e) Security enforcement.

(f) Training (including of the Customer's personnel).

(g) Software or hardware maintenance, licensing or upgrades.

(h) Internet and WAN link issues.

(i) Installation services.

(j) Digital Forensic services and Incident Response Services (sometimes referred to as DFIR).

(k) Security design and architecture.

(l) Security policy or procedure establishment.

(m) Firewall rule set design, validation and troubleshooting.

(n) Export of data to, or integration of Interactive's SIEM or other CSOC platforms with, the Customer's systems or external systems.

(o) Communicating with Customer personnel about security incidents pertaining to their identity or workstation.

(p) Assessing the Customer's Network, Server or application for signs of compromise, whether as part of the Security Incident Management Process following a Security Incident or Attack, or otherwise.

(q) Tasks associated with the resolution of a Security Incident or Attack on the IT Environment, except as set out in item 10.5(a).

(r) Expenses incurred by Interactive such as travel and accommodation, which, if required, will be charged on time and materials basis.

15 Pricing Terms

15.1 The Service Fees for the AMSOC are based on the quantity of Users, as identified in the CMS SOW.

15.2 The Customer may request to add Users by making a Service Request and providing relevant details (names and contact details). Interactive will add the User and the Customer will be charged for the addition pro-rata from the date the User is added.

15.3 The Customer may request to add Monitored Event Sources by making a Service Request and providing relevant details. Interactive will work with the Customer on a time and materials basis to design an appropriate solution and implement in line with Customer priorities.

15.4 The Customer may request to remove Users by making a Service Request and providing relevant details (names and contact details), subject to the following:

(a) the aggregate quantity of Users cannot drop below the quantity set out in the CMS SOW as at the Service Start Date;

(b) the Customer must provide at least 30 days' notice of a User deletion; and

(c) Users may only be deleted if the User's employment is terminated and the account deactivated.

15.5 If the change requested by the Customer pursuant to item 15.2 or 15.3 is acceptable to Interactive, Interactive will update the monthly report to list the current quantity of Users. The Service Fees payable will be adjusted in accordance with the reported quantities.

15.6 Service Requests made to add or remove Servers or Users will not be counted towards the 5 included Simple Service Requests per month.

15.7 If the scope increases or varies, Interactive may vary either or both of the monthly Service Fee and Implementation Fee, and the parties will enter into an addendum to the CMS SOW to reflect the variation.

16 Definitions

16.1 The following definitions apply to this AMSOC Service Description:

AMSOC Subscription Tier Table means the table set out in item 4.

Authority to Act forms part of the operations manual created by Interactive during onboarding and provides permission for Interactive to act on the Customer's behalf in order to contain and eradicate a threat.

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

Azure Managed Sentinel (AMS) Platform means the Microsoft Azure Sentinel Platform 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).

Data Quality Maturity means the improvement over time of the data which is ingested from log sources mapped against the MITRE ATT&CK Heatmap.

Detection Maturity means the improvement over time of the detections mapped against the MITRE ATT&CK Heatmap.

Endpoint Detection and Response means a product/service that alerts customers to cyber threats primarily across endpoints and can be used to perform active response measures to contain and eradicate threats.

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 (AMS) Platform.

MDR Services means the managed or endpoint detection and response services set out in the MDR Service Description. EDR Services (as may be specified in the CMS SOW) are also MDR Services.

MDR Cloud Platform refers to the distributed platform used by the MDR Service to conduct endpoint security event management.

MITRE ATT&CK Heatmap is a graphical representation of the Customer's threat detection coverage based on the MITRE ATT&CK framework.

Monitoring means the activities set out in item 9.

Monitored Event Source 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 include (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).

Network means a network that is part of or connected in some way to the IT Environment.

Operational State means, for a Monitored Event Source, where the Monitored Event Source is operational and Healthy, Functional and Tuned, as each are defined in item 5.1.

Purple Team Exercises are Cyber Threat Intelligence led attack simulations, emulating Tactics, Techniques, and Procedures (TTPs) leveraged by known malicious actors actively targeting the organisation to identify and remediate gaps in the organisation's security posture and detection and response capability of the AMSOC.

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).

Response Time means, with respect to each Security Incident, the time calculated from the time Interactive receives the alert about the Security Incident, until the time Interactive reviews the alert on its systems.

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

Security Incident means one or more Security Events identified by the Customer or Interactive to be an adverse condition or situation in the IT Environment.

Security Incident Active Response means a containment activity such as blocking a process or network connection as approved by the Customer.

Security Incident Management Process means the six phase process set out in item 10.

Server means a server in the IT Environment and **Servers** means each one of them.

Service Desk means the Interactive technical support group that acts as a single point of contact between Interactive and the Customer to manage all Security Incidents, Service Requests, communications and escalations with the Customer.

Service Levels means the Severity Levels and the Response Time Targets set out in item 10.3(b).

Service Start Date means the date determined in accordance with item 1.2

Simple Service Request is defined as a Service Request, which can be completed within 2 hours of effort and does not require representation at the Interactive change advisory board.

SOAR 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.

Subscription Tier means the level of Azure SOC Services, which may be Enhanced or Enterprise as set out in the CMS SOW and further described in the AMSOC Subscription Tier Table.

Supported Data Sources List means the Azure Sentinel supported data sources list, as may be updated or replaced from time to time, which is located at the following URL, or any updated URL: https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources or as agreed by Interactive

Threat Actor means the person or entity committing an Attack on the Customer's IT Environment.

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