CYBER SECURITY – SERVICE DESCRIPTION

Cyber Security Operations Centre as a Service (CSOC)

This Service Description ("**CSOC Service Description**") contains the terms governing the provision of the service known as Cyber Security Operations Centre as a Service 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 CSOC Service Description ("**Customer**").

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

1 Cyber Security Operations

1.1 Interactive will provide CSOC for the Individual Term. The CSOC provides the Customer with a detection and response capability, via Interactive's Security Information and Event Management (**SIEM**) platform.

2 Readiness Assessment

2.1 Interactive will, within 14 days after the Commencement Date, conduct a readiness assessment of the Customer's infrastructure to determine whether the Customer's existing infrastructure is able to support the CSOC.

2.2 Interactive will notify the Customer regarding the Operational State of a Monitored Event Source if the Monitored Event Source is found to have a negative impact on Interactive's ability to deliver the CSOC, if identified during the assessment of the Customer's infrastructure.

2.3 The Customer must make any necessary changes to the relevant Monitored Event Source to put it in an Operational State within 3 months after being informed about issues.

3 Customer Onboarding

3.1 Interactive will perform the following to onboard the Customer:

(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; and

iii. facilitate effective communication by way of updates on the progress of the Onboarding Tasks;

(b) coordinate the mutual provision of information;

(c) establish connectivity between the Customer and Interactive as described in item 5;

(d) obtain service delivery enablement as set out in item 7;

(e) provide the Readiness Assessment Document; and

(f) create a list of expected Monitored Event Sources as at the Service Start Date (that list is the "**Monitored Event Source List**"),

(Collectively, the "**Onboarding Tasks**").

3.2 The Customer must:

(a) provide a single point of contact for all Onboarding Tasks; and

(b) complete and return the onboarding pack documents within five Business Days after receiving it from Interactive.

3.3 If the Customer fails to perform obligations which are required to complete the Onboarding Tasks, the Customer acknowledges that full operation of the CSOC may be delayed.

3.4 As part of the onboarding process, Interactive and the Customer will agree on certain pre-approved actions that Interactive can perform in the event of a Security Incident.

4 Monitored Event Sources

4.1 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 log volume and ensuring redundant or unnecessary configurations are removed.

4.2 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.

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

4.4 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 CSOC.

4.5 The Customer is responsible to ensure 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.

4.6 To allow Interactive to provide the CSOC, 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 (**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.

4.7 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.

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

5 Customer Connectivity and Event Collector Deployment

5.1 Interactive will:

(a) conduct a requirement gathering exercise with the Customer to determine the most suitable connectivity design and determine the approach, timeframes and costs for connectivity implementation.

(b) establish secure communications channels between the Customer's infrastructure where the Event Collectors are hosted and Interactive's infrastructure by the way of:

i. internet based SSH tunnel; or

ii. internet-based site-to-site Virtual Private Network (VPN); or

iii. private site-to-site VPN; or

iv. secure site to site connection.

(c) provide an architecture diagram on request.

5.2 Based on the requirement gathering exercise, Interactive will determine the quantity of Event Collectors necessary. A maximum of 2 Event Collectors are included in the Service Fees. If additional Event Collectors are required (which may be, for example, if a large amount of log correlation is to be performed or overlapping Networks exist) more may be deployed as Out of Scope Work.

5.3 The Customer must perform the following as required by Interactive:

(a) Provide access to the Event Collector(s) through VPN or other secure method,

(b) Provide secure access to the Customer's logging environment in the event security analysts require additional logs during an investigation,

(c) Provide secure access to requested resources (IT systems) in the Customers IT Environment that support CSOC. and

(d) supply Interactive with:

i. copies of all existing Network documentation including risk analysis reports, policies and procedures;

ii. any customised notification and escalation procedures; and

iii. any customised change management procedures.

5.4 The Customer may use its own VPN device for the CSOC if:

(a) Interactive advises the Customer that the VPN device is suitable for the CSOC, based on Interactive's assessment of the device hardware specifications provided by the Customer; and

(b) the Customer makes any configuration changes to the Customer's VPN device that are required by Interactive.

5.5 The Customer must provide and maintain the compute (either locally or in its public/private cloud environment) for the Event Collector based on the minimum requirements as described in the Readiness Assessment Document (provided during onboarding).

5.6 The Customer must provide adequate bandwidth to enable Interactive to receive logs from Monitored Event Sources.

6 Changes to Monitored Event Sources and Event Collector

6.1 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 and/or Event Collectors;

(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 and/or Event Collectors; 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 4.4 and 6.1(a), if the Customer makes any changes without complying with item 6.1(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.

6.2 The Customer grants Interactive physical and remote access to the Event Collector, including to wipe the operating system of the Event Collector, which will preserve data integrity and separation of duties and enable sanitation post termination. This item 6.2 survives termination of the CMS SOW.

6.3 Interactive will charge the Customer for CSOC 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.

6.4 The Customer acknowledges it will not be given access to, and is not permitted to access, the Event Collector. The Customer must not pause, reboot or clone the Event Collector without Interactive's prior written approval.

7 CSOC Acceptance and Activation

7.1 After completion of the other Onboarding Tasks, Interactive will:

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

(b) provision connectivity to all Event Collectors;

(c) provide the Customer with the security operations manual;

(d) confirm receipt of log data from all Event Collectors;

(e) confirm categorisation of critical Monitored Event Sources; and

(f) generate automated reports to validate Monitored Event Source data.

7.2 On completion of the tasks in item 7.1, Interactive will notify the Customer of the date the Customer may commence conducting Acceptance Tests of those tasks ("**Acceptance Test Commencement Date**").

7.3 The Customer shall complete Acceptance Testing no later than five (5) Business Days after the Acceptance Test Commencement Date.

7.4 If the Customer's Acceptance Testing identifies any defects caused by Interactive that prevent the Customer from receiving the CSOC, 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 7.3 will apply again.

7.5 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.

7.6 If the Customer fails to complete Acceptance Testing or deliver a notice rejecting the Acceptance Tests within five (5) Business Days after the Acceptance Test Commencement Date, then Acceptance Testing will be deemed completed by the Customer. After the Customer has 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.

8 Log Processing

8.1 Interactive will collect and manage log data from the Monitored Event Sources in accordance with the following process:

(a) Collection – Event Collectors collect log data generated by the Monitored Event Sources log source;

(b) Parsing – Take the raw events from the Monitored Event Source and parse the fields into a usable format for the SIEM in use;

(c) Aggregation – the Event Collector removes duplicate Security Events to reduce large volumes of Security Event data into a manageable set;

(d) Forwarding - the Event Collector associates the events with a “customer” or a “domain” before compressing, encrypting and forwarding the logs to the Interactive management system for mining and correlation; and

(e) Event Storage - A time-series database for Security Events where data is. Data is stored on the Event Processor where the Security Event is processed.

8.2 The Event Collector sends normalised Security Event data to a processor where the Security Events are processed by custom rules engine (**CRE**) (the processor is the “**Event Processor**”). If Security Events are matched to the CRE custom rules that are predefined on the SIEM console, the Event Processor executes the action that is defined for the rule response.

8.3 Interactive will retain monthly Monitored Event Source logs for 3 months.

8.4 Interactive will retain Monitored Event Source logs for up to 12 months if requested by the Customer. The Service Fees payable for this retention are based on the total amount of storage required in GB and charged at the per GB price set out in the Cyber Security Rate Card. The Customer acknowledges pricing is based on consumption and will vary during the Individual Term.

8.5 Interactive is not responsible for any inability to deliver the log collection and storage service described in item 8.3 or 8.4 where the inability to deliver is caused or contributed to by Unauthorised Changes.

8.6 The Customer must rectify issues relating to the Monitored Event Source when the Monitored Event Source is not presenting logs to the log collection infrastructure or may engage Interactive to do so as Out of Scope Work.

9 Global Intelligence Monitoring

9.1 Interactive will utilise Threat Intelligence to enrich analysis and events within the CSOC.

9.2 Threat Intelligence is gathered from a variety of open-source data feeds as well as paid or proprietary feeds.

10 Event Monitoring

10.1 Interactive will monitor the Monitored Event Sources through a series of Detection Rules that identify Security Alerts.

10.2 Event monitoring is performed 24 hours a day, 7 days a week.

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

10.4 Interactive will include notifications obtained through monitoring as part of the Security Event Monitoring Process.

10.5 From the Service Start Date, Interactive will perform Security Alert baselining for a period of 4 weeks. Security Alert baselining is a period of time where the CSOC monitors and tunes Security Alerting to ensure a minimum number of false positives will be generated during normal Security Monitoring. During this period, the Service Levels will not apply to the Security Incident Monitoring Process.

11 Security Incident Monitoring Process

11.1 Interactive will perform the Security Incident Monitoring Process for each Security Incident. The phases of the Security Incident Monitoring Process are:

(a) Phase 1: Detect;

(b) Phase 2: Respond;

(c) Phase 3: Hunt.

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

11.3 **Phase 1: Detect**

(a) Monitored Event Sources are analysed using pre-built and in-house Detection Rules using a variety of toolsets.

(b) Monitored Event Sources are compared to patterns and heuristics in Detection Rules and if matched, a subsequent Security Alert is sent to a security analyst for review.

(c) Each Security Alert follows a set of scripted playbooks depending on the threat detected by the Detection Rules.

(d) If a Security Alert is deemed to be genuine a Security Incident, a ticket may be raised to the Customer according to the priority level in Table1.

(e) Automation is utilised wherever possible to assist in CSOC workflow.

Table 1. Incident Priority Matrix		**Impact**			
		Extensive / Widespread	Significant / Large	Moderate / Limited	Minor / Localised
Urgency	**Critical** (Event or Alert requires immediate attention; security controls may have failed)	P1	P1	P2	P3
	High (Event or Alert requires attention; security controls partially effective)	P2	P2	P3	P4
	Medium (Event or Alert requires attention; security controls mostly effective)	P3	P3	P4	P4
	Low/Informational (Event or Alert requires attention; security controls fully effective)	P4	P4	P4	P4

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

Table2. Response Time	
Priority	**Response Time**
P1	30 mins
P2	1 hour
P3	4 Hours
P4	24 Hours

(g) The following Priority Definitions apply:

Table3: Priority Definitions	
Priority	**Definition**
P1	Impact is underway or highly likely. Immediate response is required (e.g., compromised administrative credential).
P2	Likely to result in impact. Response required to identify root cause of event and attempt remediation. (e.g., threat indicator matched for command and control infrastructure).
P3	Possible impact if unattended. Investigation is required to confirm the legitimacy of the alert (e.g., malware identified on device however cleaned by endpoint agent).
P4	No impact expected however some aspects require review (e.g., significant data upload to trusted source).

(h) The following Impact Definitions apply:

Table4: Impact Definitions	
Impact	**Definition**
Extensive / Widespread	Event or Alert may be impacting the majority of the Customer environment or have the potential to do so. Examples are large scale denial of service, virus or malicious software requiring immediate containment across several IT assets. Customer business is impacted with inability to service core business needs across the enterprise.
Significant / Large	Event or Alert may be impacting a large portion of the Customer environment or have the potential to do so. Examples include compromise or outage of a core business asset, or active malicious software with the potential to further impact business operations. Customer business is impacted with some ability to service core business needs across the enterprise. Core business assets may be impacted but are

	mostly still able to provide service. A risk of further compromise is high throughout the Customer Environment.
Moderate / Limited	Event or Alert may be impacting a small portion of the Customer environment. Examples include an active phishing operation that requires attention, indicators of a possible compromise occurring in the Customer environment, or misconfiguration requiring remediation. Customer business is minimally impacted, and Customer is still able to service its business requirements. Core business assets are all available and able to provide service.
Minor / Localised	Event or Alert is not impacting the Customer environment. Examples include active scanning attempts, repeated offenses, or information events. Customer business is not impacted, but the Events or Alerts require review. Core business assets are all available and able to provide service.

11.4 **Phase 2: Respond**

(a) Each Security Alert goes through a standard triage process to build context and eliminate false positives.

(b) The steps followed for each Security Alert is as follows:

i. Triage

ii. Priority Rating

iii. Evidence Gathering

iv. Escalation to Incident

v. Threat Cleared

(c) Each stage of the response process is detailed in Table 6

Table 6: Response Process	
Stage	**Assessment**
Triage	Event assessed against all current open Security Alerts. Assessment considers criticality of asset, likelihood to cause impact and the stage of cyber-attack. The event is then assigned a priority rating of 1 – 4 according to Table1. This decides the order in which the security analyst responds to events.
Priority Ratings	Once events have been prioritised, the response can be focused on the high priority events (1) first. **P 1**: Impact is underway or highly likely. Immediate response is required (e.g., compromised administrative credential). **P 2:** It is likely impact will result. Response required to identify root cause of event and attempt remediation. (e.g., threat indicator matched for command and control infrastructure).

	P 3: Possible impact if unattended. Investigation is required to confirm the legitimacy of the alert (e.g., malware identified on device however cleaned by endpoint agent). **P 4**: No impact expected however some aspects require review (e.g., significant data upload to trusted source). Once priority ratings have been assigned, the security analyst reviews each in priority order. When each case is assessed, it is moved into evidence gathering.
Evidence Gathering	Security analysts determine the nature of the event and whether escalation to the Customer, as a Security Incident, is necessary. The necessity of an escalation is determined by an incident playbook. Each Security Alert will follow a play book depending on what the likely threat may be. The security analyst correlates evidence from other sources, tool sets and from open-source intelligence sources. If there is evidence to suggest that nefarious actors are involved, the event is escalated to a Security Incident.
Incident Management	If an Incident Response team is required, this will be treated as Out of Scope Work and a separate statement of work with Interactive may be required.
Threat Cleared	When an event or an incident has been remediated and the threat cleared – then the state is moved to closed.

(d) Interactive will monitor against Detection Rules for several Monitored Event Sources.

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

iii. copy and safely store audit trails, log files and intrusion traces from any other devices that were targeted; and

iv. notify Interactive about any changes that may impact on the CSOC.

(f) If the CMS SOW states the Customer receives MDR Services, Interactive will perform all containment and eradication activities that are available through the Cloud Platform for the MDR Services.

(g) The CSOC will endeavour to limit the impact and eradicate a Security Incident with the toolsets available.

(h) Additional Out of Scope Work may be required to engage an incident response team as required. Interactive will work with Customer to understand these options in the event of a Security Incident. If an Incident Response team is required, this will be treated as Out of Scope Work and may require a separate statement of work with Interactive.

11.5 **Phase 3: Hunt**

(a) Security analysts will utilise Threat Intelligence and previous Security Events to hunt for Security Alerts on the Customer Network.

(b) A threat hunt involves security analysts searching for indicators of compromise in the Customers IT Environment using the Monitored Event Sources.

(c) Hunts may occur when new vulnerabilities are discovered, or new Threat Intelligence is received that may pose a risk to Customer.

(d) Interactive will act in accordance with the agreed Customer operations manual.

12 Reporting

12.1 Interactive will provide a standard, system generated report each month.

12.2 Interactive will review the results of the monthly report to identify key findings, provide recommendations, and provide analyst insights to the Customer as part of the monthly report.

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

13 Attack Simulations

13.1 Attack simulations may be performed periodically throughout the CSOC service.

13.2 Attack simulations use methods employed by threat actors to test and ensure Detection Rules are working appropriately as a form of technical assurance by the CSOC.

13.3 Results of Attack simulations will be discussed in regular Reporting and meetings with Customer.

13.4 Attack simulations are performed with Customer awareness at a maximum number of one per calendar year.

14 Service Desk

14.1 Interactive will provide a Service Desk function that:

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

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

(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.

14.2 The Customer must:

(a) ensure that Security Incidents and Service Requests are only raised with the Service Desk by personnel authorised, as notified to Interactive, and who have a good understanding of the CSOC;

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

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

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

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

15 Service Requests

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

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

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

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

(d) adding a User as a recipient for future reports.

15.2 Interactive will provide the Customer with up to 5 Simple Service Requests per month. Interactive may execute on 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.

15.3 Interactive will advise the Customer if any Service Request relates to Out of Scope Work prior to executing on the Service Request. Interactive will provide a quote for consideration and approval by the Customer, before executing on any Service Requests made for Out of Scope Work.

16 Service Exclusions

16.1 The Customer agrees and acknowledges Interactive is not required to contain or eradicate any threats, vulnerabilities or Attacks, except as set out in item 11.5(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 item 11.5 to do so and the threat or vulnerability was not detected or prevented directly due to Interactive's gross negligence or intentional misconduct.

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

16.3 The CSOC does not include any of the following:

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

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

(c) Configuration of secure access to 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, connectivity and WAN link support.

(i) Installation services (with the exception of Event Collectors).

(j) Forensic services.

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

(p) Tasks associated with the resolution of a Security Incident or Attack on the IT Environment, except as set out in item 11.5(a).

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

16.4 If the SIEM capacity is exceeded, Interactive will notify the Customer. If the SIEM capacity continues to be exceeded in one or more months after the notification, additional charges will be incurred and charged in accordance with the Cyber Security Rate Card.

17 CSOC Pricing Terms

17.1 The Service Fees for the CSOC are based on the quantity of Servers and Users, as identified in the CMS SOW.

17.2 The Customer may request to add Servers or Users by making a Service Request and providing relevant details (names and IP addresses). Interactive will add the Server or User and the Customer will be charged for the addition pro-rata from the date it is added.

17.3 The Customer may request to remove Servers or Users by making a Service Request and providing relevant details (names and IP addresses), subject to the following:

(a) The aggregate quantity of Servers and Users cannot drop below 50.

(b) The Customer must provide at least 30 days' notice of a deletion.

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

(d) Servers may only be deleted if the Server has been decommissioned.

17.4 If the change requested by the Customer pursuant to item 17.2 or 17.3 is acceptable to Interactive, Interactive will update the monthly report to list the current quantity of Servers and Users. The Service Fees payable will be adjusted in accordance with the reported quantities.

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

17.6 If during completion of the Onboarding Tasks, 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.

18 Additional Service Terms

18.1 This clause applies if Microsoft Azure Sentinel is being used to provision CSOC.

(a) The Customer must agree and comply with the following terms

i. Microsoft Customer Agreement:https://learn.microsoft.com/en-us/partner-center/agreements; and

ii. The relevant Azure Sentinel terms referenced under: https://www.microsoft.com/licensing/terms

18.2 This clause applies if the Customer deploys Splunk Support Programs on its own behalf:

(a) The Customer agrees that:

i. any Content indexed using a Purchased Offering must originate only from the Customer's assets that are hosted within a data centre or cloud environment that is owned or leased (e.g., from AWS) by Interactive or the Customer;

ii. the Customer will purchase adequate Capacity to accommodate its peak daily usage; and

iii. the Customer will not use Purchased Offerings, or any portion of the Capacity associated therewith, to support any third party's business purposes.

(b) The Customer remains fully liable for any and all acts or omissions related to use of CSOC. The Customer is responsible for ensuring that any use by the Customer of the Purchased Offerings is only for the Client's Internal Business Purposes.

(c) For the purposes of this clause the following definitions apply:

i. "Content" means any data that is ingested by the Customer into an Offering.

ii. "Purchased Offerings" means the services, subscriptions and licenses to Offerings that are acquired by the Customer from Splunk directly or through an Authorized Distributor.

iii. "Offerings" means the products, services and other offerings that Splunk makes generally available for Managed Services.

iv. "Capacity" means the measurement of usage of an Offering (e.g., aggregate daily volume of data indexed, specific source type rights, number of search and compute units, number of monitored accounts, virtual CPUs, User seats, use cases, storage capacity, etc.) that is purchased for an Offering.

v. "Splunk Support Programs" are the Support Programs offered by Splunk and identified here: www.splunk.com/en_us/support-and-services/support-programs.html or such other URL as Splunk makes available for Support Programs from time to time.

19 Definitions

19.1 The following definitions apply to this CSOC Service Description:

CSOC means the Services described in this CSOC Service Description.

Detection Rule means a set of computer logic (pattern matching, heuristics, statistical) that matches one or more Security Events against suspicious behavioural patterns. Pattern matches that occur in a Detection Rule result in a Security Alert being generated by the CSOC.

Event Collector means an Interactive physical or virtual appliance or software product located at the Customer Location or cloud location that automates the process of collecting and managing logs from any Monitored Event Source and in any format, through normalisation and categorisation into a common event format for use in the delivery of the CSOC.

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

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

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

(c) 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 4.1.

Readiness Assessment Document is the document completed at the end of the readiness assessment that outlines the high-level design and connectivity of the solution.

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 CSOC, which is observed from one or more Monitored Event Sources.

Security Alert means a Security Event that met the condition of a Detection Rule and requires additional review through additional enrichment, automation, or human intervention.

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

Security Incident Monitoring Process means the process set out in item 11.

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.

Security Information and Event Management (SIEM) means software that aggregates logfiles into a single location for a security analyst to review and escalate as appropriate.

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.

Supported Vendor List means the list of supported vendor technologies supported.

Threat Intelligence means a list of data feeds that the CSOC monitor to gain proactive insight and context into Security Events and the cyber security threat landscape.

Unauthorised Change is defined in item 6.1(c).

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