MANAGED SECURITY SERVICES PROVIDER ("MSSP") AGREEMENT

THIS MSSP AGREEMENT (this "Agreement") is entered into effective as of the date signed by (the "Effective Date") between (1) XXXXXX (Registered in England & Wales with Company No. XXXXX) having a registered office address at XXXXX ("Customer"); and (2) Si Consult Ltd (Registered in England & Wales with Company No. 04850713) having a registered office address at Flat D, 4 Chelsea Embankment, Corner of Tite Street, London SW3 4LF ("Supplier") to enable the Customer to purchase Managed Security Services provided by the Supplier.

1. SERVICES.

(a) Supplier will provide Customer and its Affiliates with security network monitoring services as described on the Service Order attached as Attachment A (the "Service Order") in accordance with the terms and conditions set out in this Agreement (the "Services").

(b) Supplier will provide the Services in accordance with the service levels attached as Attachment B. Those services will be resold to the Customer by the Reseller.

(c) Customer agrees to fully cooperate with Supplier to create a VPN tunnel or similar communication conduit to Customer's and its Affilates' network as set out in the Service Order, in order for Supplier to provide the Services and subject to Customer's compliance with the aforementioned obligation the Supplier agrees to ensure the Services are being provided in full, as provided for in Attachment A, no later than 30 days after the Customer has complied with all such obligations as have been notified to it by the Supplier (failing which the Customer shall have the right, but not the obligation, to terminate the Agreement by notice with immediate effect).

2. FEES & PAYMENT TERMS.

(a) Customer will pay Supplier fees as described on the Service Order (the "Fees").

(b) Supplier will invoice Customer for the applicable Fees annually in advance.

(c) Customer will pay undisputed invoices on a net monthly basis without deduction, set-off, deferment, or counterclaim. Amounts due but unpaid shall accrue interest in at the rate of 4% per annum above the London Inter-Bank Offered Rate (administered by ICE Benchmark Administration Limited)(LIBOR) from time to time, provided that where the LIBOR rate is less than zero it shall be treated as being zero. Such interest shall accrue on a daily basis until actual payment of the overdue amount, whether before or after judgment. The Customer shall pay the interest together with the overdue amount. All amounts stated in the Agreement or on any invoice are in Pounds Sterling (GBP), and all payments will be made in the same currency. Customer will pay any VAT or other sales tax related to the Services, exclusive of taxes on Supplier's income.

3. TERM & Renewals. The initial term of this Agreement begins on the Effective Date and shall end One (1) years after the Service Start Date (the "Initial Term"), unless terminated earlier as provided in the Agreement. Upon expiry of the Initial Term and each Renewal Term (as defined below), the term of the Agreement shall automatically renew for one (1) year renewal term (each, a "Renewal Term"), provided that either party may elect not to renew the term of the Agreement by providing the other party with written notice of the non-renewal at least forty five (45) days prior to the beginning of the upcoming Renewal Term.

4. TERMINATION. (a) In the event that a party commits a material breach of this Agreement (including, but not limited to, any failure by Customer to pay any Fees by the applicable due date), the non-breaching party may terminate this Agreement on thirty (30) days' prior, written notice to the breaching party; provided, however, that this Agreement will not terminate if such breach is cured within such thirty (30) day period.

(b) Either party may terminate this Agreement forthwith by notice if the other party becomes insolvent on any basis, or suspends or threatens to suspend or ceases to carry on all or a substantial part of its business, or if it takes or gives notice that it intends to take, or it becomes subject to, any steps in any form of insolvency, winding up, administration or receivership process.

5. EFFECT OF TERMINATION. (a) The provision of the Services shall end immediately upon any termination of this Agreement and Customer shall immediately cease any use of the Services upon such termination either in accordance with Section 3 or Section 4.

(b) The following provisions shall survive any termination or expiry of this Agreement: this Section 5 ("Effect of Termination"), Section 6 ("Restrictions on Use"), Section 7 ("Intellectual Property Rights"), Section 8 ("Confidentiality"), Section 9 ("Representations and Warranties; Disclaimer"), Section 10 ("Limitation of Liability"), Section 11 ("Indemnification") and Section 12 ("Miscellaneous").

(c) Upon termination of this Agreement the Supplier will, at Customer's request, cooperate in effecting such arrangements, including by executing and delivering or doing, as appropriate, all such documents, assurances and acts as Customer may reasonably request in order for Customer to enter into a contract with Si Consult Ltd for the provision of the Services by Si Consult Ltd directly or any other third party to Customer.

(d) If Customer terminates this Agreement under section 4 Supplier shall reimburse Customer the remaining Fees previously paid in respect of the annual Term during which the Agreement is terminated.

6. RESTRICTIONS ON USE. (a) Customer shall not, and shall procure that its Affiliates shall not, use the Services other than for lawful purposes in connection with the monitoring of Customer's computer networks. Customer shall not, and shall procure that its Affiliates and its and their respective employees, agents and contractors (collectively, its "Representatives") shall not decompile, disassemble, reverse engineer, copy, modify or permit any third party to access or use any software provided or used by Supplier or any of its licensors or service providers in connection with the provision of the Services except to the extent that (by virtue of section 296A of the Copyright, Designs and Patents Act 1988) such actions cannot be prohibited because they are essential for the purpose of achieving inter-operability of the software with another software program, and provided that the information obtained by Customer or its Affiliates during such activities (i) is used only for the purpose of achieving inter-operability of the software with another software program, and is not unnecessarily disclosed or communicated to any third party without Supplier's prior written consent, and is not used to create any software which is substantially similar to any of the software provided.

(c) Customer acknowledges and agrees that the Services have been designed and tested for use in ordinary business environments and not for use in any high-risk applications, including the operation of nuclear facilities, aircraft navigation, air traffic control, emergency communications systems, life support machines, weapons systems, or any other application where the failure, interruption, inadequacy or malfunction of the Services can reasonably be expected to result in death, personal injury, severe property damage or severe environmental harm ("High Risk Applications"). The Services are not fault-tolerant and are not designed or intended for use in, and Customer shall not, and shall procure that its Affiliates shall not, use any Services in, any hazardous environments requiring fail-safe performance or in any High Risk Applications. Customer shall not, and shall procure that its Affiliates shall not, resell the service.

(d) Customer shall not, and shall procure that its Affiliates shall not, export, directly or indirectly, any software or technical data acquired from Supplier or any of its licensors or other third party service providers under this Agreement in breach of any applicable laws or regulations to any country for which the UK government or any agency thereof at the time of export requires an export licence or other governmental approval without first obtaining such licence or approval.

7. INTELLECTUAL PROPERTY RIGHTS. No intellectual property rights of any kind are assigned or transferred to Customer or any of its Affiliates under this Agreement. Customer shall not (and shall procure that none of its Affiliates, Representatives or Representatives of its Affiliates shall) challenge, or assist any person or entity in challenging, the right, title, and interest of Supplier or any of its licensors or service providers in and to the Services and any software or other technology used in the provision of the Services. Customer and its Affiliates are granted a personal non-transferable, non-exclusive licence to use such intellectual property rights if and to the extent that and for so long as such use is necessary in order for Customer and its Affiliates to lawfully receive the benefit of the Services in accordance with this Agreement.

8. CONFIDENTIALITY AND DATA PROCESSING.

8.1. Confidentiality

(a) "Confidential Information" means all information provided by or on behalf of a party (the "Disclosing Party") to the other party (the "Receiving Party") hereunder that consists of proprietary and/or non-public information relating to the past, present or future business activities of the Disclosing Party or its Affiliates, including, but not limited to, information relating to the Disclosing Party's or any of its Affiliate's business plans, pricing, financial information, methods, processes, software (including source code and object code), data, information technology, network designs, passwords, and sign-on codes. For the avoidance of doubt, Confidential Information of Supplier includes, without limitation, any software or software configuration used in the provision of the Services, as well as the pricing set out in this Agreement (including the Service Order) and shall include Personal Data.

(b) Notwithstanding the foregoing, Confidential Information does not include information which: (i) is or becomes public knowledge without any action by, or involvement of, the Receiving Party; (ii) is disclosed by the Receiving Party with the prior written approval of the Disclosing Party; (iii) is independently developed by the Receiving Party without use of Confidential Information; or (iv) is intentionally disclosed by the Disclosing Party to a third party without restriction on disclosure.

(c) The Receiving Party agrees: (i) not to disclose the Disclosing Party's Confidential Information to anyone other than its employees and contractors who have a need to know such Confidential Information; (ii) not to use or exploit such Confidential Information, except as required to perform its obligations under this Agreement; and (iii) to ensure that any of its employees and contractors who receive access to such Confidential Information are advised of the confidential and proprietary nature thereof and are prohibited from copying, using or disclosing such Confidential Information, except as required to perform any obligations under this Agreement.

(d) Receiving Party agrees to employ with regard to the Confidential Information procedures that are no less rigorous and secure than the procedures used by it to protect its own confidential and proprietary information of similar sensitivity (and in any event that in no event are less rigorous and secure than reasonable procedures).

(e) If the Receiving Party is required to disclose any of the Disclosing Party's Confidential Information pursuant to any judicial or governmental order or by a relevant regulatory authority of mandatory and binding effect on the Receiving Party, the Receiving Party will, to the extent reasonably and legally feasible, give the Disclosing Party written notice of the request and opportunity to contest the order prior to disclosing such Confidential Information.

8.2. Data Protection

8.2.1 For the purposes of this Agreement, the Customer is the Data Controller, and the Reseller and Supplier are Data Processors. The Reseller and Supplier agree to, and agree to procure that they comply with the requirements of the Data Protection Act 2018 and General Data Protection Regulation (GDPR) and shall:

(a) unless required to do so by law (in which case they shall inform the Customer of that requirement before processing unless such law prohibits the same on important grounds of public interest) process all Personal Data only in accordance with the written instructions of the Customer and in accordance with the terms of this Agreement for the performance of its obligations pursuant to this Agreement;

(b) take appropriate technical and organisational measures against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data and that, having regard to the state of technology development and the cost of implementing any measures, such measures shall ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);

(c) take steps to ensure the reliability of any of its Representatives or Affiliates who have access to the Personal Data and ensure that they are informed of the confidential nature of the Personal Data and that they comply with the DPA when dealing with the subject matter of this Agreement

(d) co-operate with the Customer to enable the Customer to take reasonable steps to monitor compliance by the Reseller and Supplier with its obligations under this Agreement;

(e) forward to the Customer within five working days of receipt any requests from an individual for access to their Personal Data;

(f) notify the Customer immediately of any correspondence received from the Information Commissioner's Office relating to Personal Data or any complaint from an individual about the processing of their Personal Data;

(g) not to transfer, or cause or permit the transfer, of any Personal Data outside the European Economic Area ("EEA") without the Customer's prior written consent; and

(h) not to do or omit to do anything which would cause the Customer to be in breach of the DPA.

8.2.2. The Supplier and Reseller confirm to the Customer that any notification required under the DPA is accurate, up-to-date and complete and permits the processing of Personal Data.

8.2.3. The Reseller and Supplier shall, and shall procure that each Third Party Service Provider shall, be contractually bound by provisions no less onerous that those contained in this Clause 8 in relation to Data Protection. The Reseller and Supplier shall be jointly and severally liable for all acts and omissions by any third party entity, including but not limited to each Third Party Service Provider.

8.2.4. The Reseller and Supplier shall, and shall procure that each Third Party Service Provider shall, observe and comply with all information technology requirements, together with all of the Customer's applicable standards and / or policies as notified by the Customer from time to time. The Reseller and Supplier shall not, and shall procure that each Third Party Service Provider shall not, damage or corrupt Customer systems and / or data (including but not limited to Personal Data) and shall comply with the Customer's Information Security Requirements.

8.2.5. The Reseller and Supplier represent and warrant that all Personal Data shall only be transferred, stored, located and processed in the United Kingdom,unless the parties agree in writing otherwise (in writing for the purposes of this Agreement does not include email).

The Reseller and Supplier shall not transfer any Personal Data to any Third Party Service Provider without the prior written consent of the Customer.

The Reseller and Supplier shall promptly and in any event within 30 days of the date of cessation of any Services involving the Processing of the Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Customer Personal Data.

The Reseller and Supplier shall notify the Customer without undue delay upon becoming aware of a personal data breach affecting the Personal Data (or with any sub-processor), providing the Customer with sufficient information to allow the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the DPA. The Reseller and Supplier shall co-operate with the Customer and take such reasonable steps as are directed by the Customer to assist in the investigation, mitigation and remediation of each such personal data breach.

The Reseller and Supplier shall make available to the Customer on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of the Customer Personal Data by them.

9. REPRESENTATIONS AND WARRANTIES; DISCLAIMER.

(a) Each party represents and warrants that it has the full right, power and authority to enter into this Agreement and to discharge its obligations hereunder. Without limiting the foregoing, Customer represents and warrants to Supplier that it has all required authority to permit Supplier and its sub-contractors and affiliates to access and monitor Customer's network and provide the Services in accordance with this Agreement.

(b) The Supplier warrants to the Customer that the Services will be provided in accordance with and on the basis of the specification set out in Attachment A and will be provided with in accordance with reasonable skill, care and diligence and good industry practice.

(c) The Supplier warrants to the Customer that the Software will be delivered free from vulnerabilities, viruses and other malicious code adnd that the Software has not included or used any open-source software or any libraries or code licensed from time to time under the gnerla public licence (as those terms are defined by the Open Source Initiative orthe free software foundation) or anything similar in, in the development of, the software, nor does the software operate in such a way that it is compiled with or linked to any of the foregoing.

(d) The services are provided on an "as is" and "as available" basis. except as set out in sections 9(a),(b) and (c) above, supplier and its third party service providers disclaim any and all implied warranties of merchantability, fitness for a particular purpose, satisfactory quality, skill and care, non-infringement, error-free or uninterrupted operation outside of supplier control i.e. force majeure.

(e) Without limiting the foregoing, neither supplier nor any of its licensors or service providers makes any representation or warranty that save to the extent required to comply with the terms of this agreement. to the extent that supplier and/or its service providers may not as a matter of applicable law disclaim an implied warranty or condition, the scope and duration of such warranty or condition will be the minimum permitted under such law.

10. LIMITATION OF LIABILITY. (a) Nothing in this Agreement limits or excludes Supplier's liability for death or personal injury resulting from its negligence, fraud or fraudulent misrepresentation, breach of the obligations implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of the Goods and Services Act 1982, or any other liability that cannot be excluded or limited by English law. All other provisions of this Agreement including in this section 10 are subject to the foregoing,

(b) Neither party nor any of its service providers will be liable to the other party (nor to any other person claiming rights derived from the other party's rights) for consequential, incidental, indirect, punitive, special or exemplary losses or damages of any kind or for any loss of revenues, loss of profits, loss of cost or other savings, loss of goodwill or reputation or (in each case whether direct or indirect loss or damage) with respect to any claims based on contract, tort or otherwise (including negligence and strict liability) arising from or relating to the services or otherwise arising out of or in connection with this agreement, and regardless of whether either party or any of its service providers was advised of, had other reason to know, or in fact knew of the possibility thereof. To the extent that any of the foregoing exclusions of liability is not permitted under applicable law, each Party and its service providers' liability in such case will be limited to the greatest extent permitted by law.

(c) Each party and each of its service providers' maximum liability arising out of or in connection with the services or otherwise arising out of or in connection with this agreement, regardless of the cause of action (whether in contract, tort, breach of warranty or otherwise), will in no circumstances exceed an amount equal to 1.5 times the annual fees actually paid to the supplier by the customer.

11. NOT USED.

12. MISCELLANEOUS.

(a) Relationship of the Parties. Each Party is an independent contractor of the other Party. Nothing herein will constitute a partnership between or joint venture by the Parties, or constitute either Party the agent of the other.

(b) Entire Agreement. This Agreement contains the entire understanding of the parties with respect to the subject matter hereof and supersedes all prior agreements and commitments with respect thereto. There are no other oral or written understandings, terms or conditions with respect to the subject matter of this Agreement, and neither party has relied upon any representation, express or implied, not contained in this Agreement. Any use of either party's pre-printed forms, such as purchase orders, are for convenience only, and any pre-printed terms set forth therein that are in addition to, inconsistent or in conflict with the terms of this Agreement shall be given no force or effect.

(c) Governing Law. This Agreement shall be governed by and construed in accordance with English law.

(d) Exclusive Forum. The parties hereby irrevocably submit to the exclusive jurisdiction of the Courts of England and Wales.

(e) Waiver. The rights and remedies of the parties are cumulative. No waiver of any rights shall be binding on any party unless such waiver is in writing signed by an authorised representative of the party so charged. Neither the failure nor any delay by any party in exercising any right, power, or privilege under this Agreement will operate as a waiver of such right, power, or privilege, and no single or partial exercise of any such right, power, or privilege will preclude any other or further exercise of such right, power, or privilege or the exercise of any other right, power, or privilege.

(f) Modification. No modification of or amendment to this Agreement will be effective unless in writing signed by authorised representatives of both parties.

(g) Severability. If any provision of this Agreement is held invalid or unenforceable by any court of competent jurisdiction, the other provisions of this Agreement will remain in full force and effect, and, if legally permitted, such offending provision will be replaced with an enforceable provision that as nearly as possible effects the parties' intent.

(h) Force Majeure. Nonperformance of either party shall be excused to the extent that performance is rendered impossible by strike, fire, flood, governmental acts, orders or restrictions, failure of suppliers or other third parties, network outage, environmental outage, or any reason where failure to perform is beyond the reasonable control and not caused by the negligence of the non-performing party provided that should such excused nonperformance continue for a period in excess of 90 days either party shall have the right to terminate this agreement immediately by giving notice to the other party.

(i) Assignment. Customer may not assign or otherwise transfer any of its rights or obligations under the Agreement without the express prior written consent of Supplier, (not to be unreasonably withheld or delayed). Supplier may freely transfer or assign its rights and obligations under the Agreement, in whole or in part, with the consent of Customer (not to be unreasonably withheld or delayed): (i) to any of Supplier's affiliates or (ii) in connection with any merger, consolidation, sale of equity interests, sale of all or substantially all assets, or other change of control transaction involving Supplier or the part of Supplier's business to which this Agreement relates. Subject to the foregoing, the Agreement will be binding upon and inure to the benefit of the parties hereto and their permitted successors and assigns. Any purported or attempted assignment or other transfer or delegation in violation of this Section shall be null and void.

(j) Not used.

(k) Non-Solicitation. During the term of this Agreement and for twelve (12) months thereafter, neither party shall solicit, induce or encourage any employee or consultant of the other party or any of its affiliates or service providers to accept an offer of employment or other engagement. The restrictions set forth in this Section shall not apply to individuals hired or otherwise engaged as a result of a general solicitation (such as a newspaper, radio, web or television advertisement) not directed specifically to employees or consultants of either party or any of their affiliates, or on the independent recommendation of a third party recruiter.

(l) Third Party Rights. Supplier's licensors and third party service providers shall be entitled to directly enforce and receive the benefit of all provisions of this Agreement which confer rights or benefits upon them or any of them including under sections 5(c), 6(a), 6(b), 7, 10, 11 and 12. Subject to the foregoing, a person who is not a party to this Agreement shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of it, but this does not affect any right or remedy of a third party which exists, or is available, apart from that Act.

(m) Regulatory Compliance. Customer shall use the Services including SecurityHQ Incident Management Platform and shall perform its obligations under this Agreement in compliance with all applicable regulatory requirements and without prejudice to the generality of the foregoing shall process all personal data in accordance with the Data Protection Act and shall comply with all applicable laws, regulations, codes and sanctions relating to anti-bribery and anti-corruption including but not limited to the Bribery Act 2010.

(n) Headings. The section titles in this Agreement are for convenience only and have no legal effect.

(o) Interpretation. In this Agreement:
(i) All references to sections and attachments are, references to sections of and attachments to this Agreement, and all attachments to this Agreement shall form part of this Agreement and any reference to this Agreement shall include the attachments. In the event of a conflict between a term of the sections and the term of an attachment to this Agreement the term of the section shall prevail.
(ii) A reference to one gender shall denote all genders and a reference to the singular shall include the plural and vice versa.

(iii) References to statutory provisions shall be construed as references to those provisions as amended, consolidated, extended or re-enacted from time to time.
(iv) References to a "company" shall be construed so as to include any company, corporation or other body corporate, wherever and however incorporated or established; references to a "person" shall be construed so as to include any individual, firm, company, government, state or agency of the state or any joint venture, association or partnership (whether or not being separate legal personality).
(v) Where the words include(s), including or in particular are used in this Agreement, they are deemed to have the words "without limitation" following them. Where the context permits, "other" and "otherwise" are illustrative and shall not limit the sense of the words preceding them.

13. Definitions
A number of definitions are provided within the preceding clauses of the Agreement; those terms which are not defined within the preceding clauses of the Agreement are defined below.

"Affiliate" means, in relation to a Party, any other entity, which directly or indirectly controls, is controlled by, or is under direct or indirect common control with, that Party from time to time.

"Data Controller" and "Data Processor" have the meanings set out in the DPA.

"Data and Processing" have the meanings set out in the DPA and the term "processed" shall be construed accordingly.

"DPA" means the Data Protection Act 2018 and the General Data Protection Regulations 2016, and including any subordinate legislation made under them, and any provisions amending, superseding or re-enacting them (whether with or without modification).

"EU Model Clauses" the standard contractual clauses that the European Commission have issued to provide adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of corresponding rights. The current clauses are issued pursuant to the following decisions 2001/497/EC; and 2004/915/EC; and 2010/87/EU, as may be further superseded or amended.

"Fees" means the charges payable for the Services by the Customer to the Reseller as more particularly set out in the Statement of Work.

"Intellectual Property Rights" means (i) copyright and rights in the nature of copyright, patents, rights in semi-conductor chip topographies, internet domain names and website addresses and other similar rights or obligations database rights and rights in trade marks, designs, know how, trade secrets, moral rights, know-how and Confidential Information (registered or unregistered); (ii) applications for registration, and the right to apply for registration, for any of these rights; and (iii) all other intellectual or industrial property rights and equivalent or similar forms of protection (and any licences in connection with any of the same) whether or not registered or capable of registration existing anywhere in the world.

"Personal Data" means any personal data (as defined in the DPA) which is subject to or intended to be subject to processing by the Data Processor pursuant to instructions given by the Data Controller.

"Representatives" means:

in the case of a company, the directors, officers, employees, agents, auditors, professional advisers, contractors and sub-contractors of the company; and

in the case of a society, the directors, officers, employees, agents, auditors, professional advisers, contractors and sub-contractors of the society.

"Service Start Date" the date on which the Services start being provided in full, as provided for in Attachment A, which will be confirmed by way of a "Go Live Notification" issued by the Supplier to the Customer.

"Software" means the software as identified in the Statement of Work, user documentation in respect of such software and any Modification which is provided to the Customer as part of the Services.

"Third Party Service Provider" means a third party that provides part or all of the Services, and is accepted by the Customer, including but not limited to IBM QRadar.

13. Marketing Support
Si may disclose Customer by name and logo as a customer of Si and to copy, exhibit, publish or

distribute any Testimonial which may be agreed for purposes of publicizing The Company's programs or for any other lawful purpose. These statements may be used in printed publications, multimedia presentations, on websites or in any other distribution media.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their duly authorized representatives.

By: Si Consult Ltd

Print Name: __________________________

Title: _______________________________

Date: _______________________________

By: CUSTOMER

Print Name: __________________________

Title: ________________________________

Date: ________________________________

Attachment A
Service Order

1 Scope of Work Table

[insert]

2 Fee Remuneration

[insert]

Attachment B
Service Level Agreement

Table of Contents

3 Introduction

3.1 Purpose

The purpose of this policy is to describe and define the Service level agreement (SLA) for MSS SOC operations.

3.2 Scope

This document applies to all of the Customer requirements listed in the customers formal requirements document.

4 Policy

A service-level agreement (SLA) is a contractual agreement outlining a specific service commitment made between contracting parties. The SLA includes a description of the overall service and service delivery within the agreed duration. The SLA may specify the levels of availability, serviceability, performance and operation.

4.1 Certain Definitions

"Event": A log message from the customer tools, or a series of log messages that are correlated by the SIEM tools into a correlated event, which may have a varying degree of criticality or relevence.

"Incident": An escalation "Incident" is defined as a correlated Event that occurs in the Customer environment being monitored by the SecurityHQ & QRadar based on the agreed security use cases, and is reported by various devices from Customer's network.

"Priority": The incident priority is assessed by the SOC in terms of the impact on the Confidentiality of Data, the Integrity of Systems and the Availability of Services and Systems, this is defined by the CIA Score and the corresponding priority is determined by the highest individual CIA score from each of the 3 individual CIA elements, as follows:

CIA Score	Priority	Confidentiality of Data	Integrity of Systems	Availability of Services and Systems
1	Informational	No Impact	No Impact	No Impact
2	Informational	May contribute to data loss if further vulnerabilities are exploited.	May contribute to system modifications if further vulnerabilities are exploited.	May contribute to system availability, if further vulnerabilities are exploited.
3	Informational			
4	Minor	Has potential to lead to data loss if unmitigated.	Has potential to lead to system modification.	Has potential to cause service availability issues, if unmitigated.
5	Minor			
6	Minor			
7	Major	Is likely to lead to data loss if unmitigated.	Is likely to lead to result in system modification if unmitigated.	Is likely to lead to cause service availability issues, if unmitigated.
8	Major			
9	Critical	Potential, undefined loss of data, outside of the business	Significant system modification and loss of integrity.	Significant or partial loss of availability of system or service.
10	Critical	Complete loss of data, outside of business	Complete loss of control	Complete loss of services, outage, denial of service

Priority 1 (P1): Critical
Priority 2 (P2): Major
Priority 3 (P3): Minor
Priority 4 (P4): Informational

“Periodic Reports”: Periodic reports are security monitoring reports delivered weekly/monthly and quarterly, as per section 3 of this Schedule.

“Mean Response Time Interval”: The arithmetic mean (calculated over a calendar month) interval of time between: (i) the time that a particular type of Incident (i.e., either “Critical” or “Major”) is displayed on the SOC monitoring panel and (ii) the time when notice of such Incident is provided to Customer by email or telephone.
“MSS Platform” is the IBM QRadar SIEM owned by the Supplier as per the terms of the agreement.

4.2 Incident Detection and Response

The Supplier shall warrant the performance of the SLA against service credits which may be deductible against invoices in the unlikely event of an SLA breach. This SLA shall cover the following 3 x critical elements:

- Incident Notification
- Incident Resolution/Response/Escalations
- Changes

4.3 Incident Notifications

RESPONSE TIME SERVICE LEVEL. The Supplier will use all commercially reasonable efforts to achieve, for each calendar month, the Mean Response Time Intervals set forth in the following:

Priority Level	Priority Descriptor	Mean Response Time Interval for Notification
1	Critical	15 minutes
2	Major	45 minutes
3	Minor	120 minutes
4	Informational	No time stipulated

4.4 Incident Resolution/Response/Escalations

INCIDENT RESOLUTION, RESPONSE & ESCALATION PROCEDURES: Post incident notification shall result in a set of activities which are focused on resolving the incident as per the defined incident response roles and responsibilities.

The resolution may be a team based activity between the Supplier and Customer and the workflow status shall be monitored in SecurityHQ, the incident management platform. The Critical Incidents and Major Incidents that are not otherwise resolved will be automatically escalated (using functionality provided by the MSS platform) as set forth in the following table. The Incident response resolution RACI matrix provides the subdivision of responsibilities for incident resolution.

Priority Level	Priority Descriptor	Resolution	Escalation
1	Critical	2 hours	Within 4 hours of problem being reported by authorised parties and/or MSS platform and still active
2	Major	4 hours	Within 8 hours of problem being reported by authorised parties and/or MSS platform and still active
3	Minor	8 hours	Within 24 hours of Incident being reported by authorised parties and/or MSS platform and still active
4	Informational	Not resolution time defined for Informational	

4.5 Incident Response Resolution RACI Matrix

Incident Response (IR) and Resolution requires mutual coordination across each stage of an IR workflow. With reference to NIST, Computer Security Incident Handling Guide (pub. #: 800-61) and the SANS IR methodology, it is important to be clear on the roles within this process. As such the following IR Stages and responsibilities are defined.

Responsible:	Those responsible for the performance of the task. There should be exactly one person with this assignment for each task.
Assists:	Those who assist completion of the task
Consulted:	Those whose opinions are sought; and with whom there is two-way communication.
Informed:	Those who are kept up-to-date on progress; and with whom there is one-way communication

IR Stage	Supplier	Customer
Preparation It's at this stage that you develop the formal incident response capability. It's at this stage where you create an incident response process defining the roles and responsibilities and procedures, defining: The right people / skill set. The criteria do declare an incident. The tools to handle an incident. What you are going to report. To whom are you going to communicate?	**Assist** We can support with sample run books and advise on the plan.	**Responsible** Customer is responsible for creating, owning the internal process for incident handling.
Detection / Identification: This is the step where you determine if an incident has occurred. Based on Events observation, indicators, you look for deviations from normal operations. You look for malicious acts or attempts to do harm.	**Responsible** Si Consult will be primarily responsible for this phase based on Incidents and Events which are detected with the monitoring tools: Correlated Violation Dashboard Anomaly Threat Hunting Observations arising from Weekly Reporting	**Assist, Consulted & Informed** Customer have a responsibility to advise Si Consult SOC of any suspicious Events or observation which become apparent based on their own observations or reports from end users.
Containment: This consists of limiting the damage. Stop the bleeding. Stop the attacker. It's where you make decision on which strategy you will use to contain the incident bases on your processes and procedures.	**Assist & Consulted** Si Consult can support with Machine Isolation (workflow process to be agreed), if this option is selected. Or otherwise we may agree on points of containment using script automation, to be confirmed as part of the agreed incident escalation matrix, during the project phase.	**Responsible** It's where you engage the business owners and decide to shut down the system or disconnect the network or continue operations and monitor the activity. All depends on the scope, magnitude and impact of the incident.
Remediation/Eradication: Removing the cause of the incident. In the case of a virus incident it may simply require removing the virus. On other	**Assist & Consulted** During the eradication phase, further investigation is often required to determine the	**Responsible** Customer is responsible for eradication, patching of vulnerabilities.

IR Stage	Supplier	Customer
complex incident cases you might need to identify and mitigate exploited vulnerabilities. It’s on this step that you should determine how it was initially executed and apply the necessary measures to ensure don’t happen again.	timeline of the incident and if possible the root cause. This is done via log analysis. If Forensics are required, this is currently outside of the scope of works.	
Recovery It means back in production. Eventually, restoring a backup or re-image a system. It’s where you return to normal operational status.	**Assist & Consult** After successful restoration it is important to monitor it for a certain time period for any reinfection or continued suspicious activity with the host.	**Responsible** This is primarily a function of the Customer IT Administration team.
Lessons Learned: Follow up activity is crucial. It’s where you can reflect and document what happen. Where you can learn what failed **and** what worked.	**Responsible** Identify improvements for detection if appropriate.	**Responsible** Identify improvements for your incident handling processes and procedures

4.6 Change Management

4.6.1 Change Priority

Priority	Change Type	Description
P1	Emergency	• Emergency fix from Third Party • Response to Security threat • Response to System - Critical Asset
P2/P3	Planned	• Update – Minor • Upgrade – Major
P3	Routine	• Access control list update, role management

4.6.2 Change Execution Target Time

Priority	Change Type	Target Lead Time	
		Evaluation (Hrs)	Execution (Hrs)
P1	Emergency	4	4
P2	Planned - Major	120	120
P3	Planned - Minor	72	72
P3	Routine	72	72

4.6.3 Change Orders Allowance

Change Type	Change Units per CI*/month	Change Period Units
Emergency	1	Month
Planned- Minor	2	Month
Planned- Major	1	Quarter
Routine	3	Month

4.6.4 Incident Related Communication

The Supplier will provide all Incident-related communications to Customer via the following means:

1. Through SecurityHQ portal;

2. Email to Customer’s designated email address;

3. Call to Customer’s designated telephone number

4.7 Reporting

For the Managed SOC services the following reporting is provided as per the standard SLA.

Report Type	Frequency	Typical Content
Daily Reports	9:00am each working day	Automatically scheduled reports from SIEM as per customer requirement.
Weekly Reports	Weekly. Day to be agreed	Manually compiled reporting with interpretive analysis. - Cyber Alert Indicator - Incident Detail Matrix - Tickets Opened & Closed - Service Request Details Report - Detailed Event Analysis Report - IP Traffic Analysis Report - Malware Analysis Report - Observations & Recommendations
Monthly Reports	Monthly. Day to be agreed	Manually compiled reporting with interpretive analysis. - Executive Summary - Cyber Alert Indicator - Incident Detail Matrix - Tickets Opened & Closed - Service Request Details Report - Detailed Event Analysis Report - IP Traffic Analysis Report - Malware Analysis Report - Network Threat Report - Endpoint Threat Report - Privilege User Threat Report - Log Volume Status - Compliance Reporting (ISO27001) - Observations & Recommendations
Incident Reports	As per SLA	These shall be generated based on notifiable P1 & P2 security incidents. This shall include a forensic diagnosis of the Incident occurrence, root cause and the mitigation requirements. P3 & P4 Incident shall be captured as part of the regular reporting, as described above.

4.8 Availability

The Supplier shall provide the Services in accordance with the following levels of availability.

Impact	Solution Component	Scheduled Down Time/ Month [A]	Restore time [B]	Total Down Time/ Month (Assume 2 [C] crashes/mth) (A) + (B*C)
High	SOC Team Availability for Analysis	None	None	None
Medium	Web SecurityHQ Portal DB	7.3 hrs	30 mins	8.3 hrs
Medium	SIEM Tool	7.3 hrs	30 mins	8.3 hrs

The log collector software deployed into the Customer environment are dependent on the availability of Customer's infrastructure, which are typically hosted on a customer virtual machine or hardware. The Supplier therefore does not warrant the performance of log collectors which are hosted in Customer's environment.