SPECIFIC CONDITIONS N1 – SECURITY MONITORING AND CONSULTANCY SERVICES

These Specific Conditions govern the Security Monitoring and Consultancy Services that may be provided by the Company under an Order Form, together with any other document or terms and conditions referred to in the Order Form including but not limited to the General Terms and Conditions for the Supply of Products and/or Services (the "**Conditions**") and Specific Conditions X3 – Standard Operational Services, which shall be deemed to be incorporated into the Contract for the performance of any Security Monitoring and Consultancy Services performed under these Specific Conditions.

1 DEFINITIONS

1.1 Capitalised terms used in these Specific Conditions shall have the following meanings for the purposes of these Specific Conditions only:

"API"	means application programming interface;
"Application"	means any security application or agent required for specific functionality of the Security Monitoring and Consultancy Services, to be installed on End User devices or server estate;
"Asset"	means a server, network, or End User device within the Customer Environment;
"Customer Environment"	means the Customer devices and infrastructure which the Platform will interact with, report on, or protect, as agreed by the parties;
"Cyber Threat"	means any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), organisational assets, or individuals through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service;
"Logs"	means a record of security information created by a device within the Customer Environment and analysed by the SIEM Platform;
"Log Collector"	means a virtual or physical machine that is responsible for collecting Logs from devices and infrastructure within the Customer Environment and forwarding them to the SIEM Platform;
"Log Source"	means a device or infrastructure within the Customer Environment that has been configured to send Logs to the Log Collector;
"Malicious Content"	means any type of malware, ransomware, spyware, adware, scareware, virus, worm, Trojan horse, or other computer program, software code, or technique used to infect, damage, disable, or disrupt computer operation, gather, erase, or encrypt data or information, or gain access to private computer systems;
"Managed SIEM"	means the service to manage the SIEM Platform provided to the Customer by the Company and defined in paragraph 3 of these Specific Conditions, if detailed in the Order Form;
"PCI DSS ASV Scanning"	means the Services provided to the Customer by the Company as detailed in paragraph 6 of these Specific Conditions, if detailed in the Order Form;
"Platform"	means the SIEM Platform and/or the Vulnerability Platform;
"Recommendation Report"	means a report provided to the Customer following an identified Security Incident or Vulnerability comprising overview, severity level, potential impact, affected devices, recommended action and further reading;
"Security Awareness and Training Services"	means the Services provided to the Customer by the Company as detailed in paragraph 7 of these Specific Conditions, if detailed in the Order Form;
"Security Incident"	means a cyber security incident relating to the Customer Environment as detected by a SIEM Platform and assessed by the Company Personnel;
"Security Incident Response Matrix"	means a written plan which includes a defined list of individuals that the Company will contact in the event of a Security Incident;
"Security Monitoring and Consultancy Services"	means collectively any of the services provided to the Customer by the Company described in these Specific Conditions;
"SIEM Platform"	means the Customer provided security information and event management platform intended to categorise, identify, and analyse security alerts related to the Customer Environment;
"Threat Model"	means a report of the Customer Environment which identifies the Assets, applications and devices most vulnerable to a Security Incident;
"VMaaS Cloud Services"	means the products and/or services, including any data, that are used by the Company in the provision of Vulnerability Management as a Service and made available online by the Vendor, including any offline components;
"Vulnerability"	means a weakness discovered in the software or firmware of a virtual or physical device which could potentially be exploited by an attacker to affect the confidentiality, integrity or availability of systems, applications and/or data;
"Vulnerability Management as a Service"	means the Services provided to the Customer by the Company as detailed in paragraph 5 of these Specific Conditions, if detailed in the Order Form;
"Vulnerability Platform"	means the Vulnerability Scanning platform intended to identify and analyse security vulnerabilities in the Customer Environment;
"Vulnerability Scan"	means an automated scan of a Customer Environment completed as a scheduled or ad hoc activity with the aim of identifying configuration weaknesses or missing security patches at a single point in time;
"Vulnerability Scanner"	means a device installed into the Customer Environment and controlled by the Vulnerability Platform in order to complete a Vulnerability Scan of the Customer Environment; and
"Vulnerability Management"	means the Services provided to the Customer by the Company and defined in paragraph 4 of these Specific Conditions, if detailed in the Order Form.

1.2 All other capitalised terms, which are not defined in paragraph 1.1 shall have the meanings stated in the Conditions and/or in Specific Conditions X3 – Standard Operational Services.

2 COMMENCEMENT DATE AND MINIMUM TERM

2.1 The Commencement Date of the Security Monitoring and Consultancy Services shall be the date specified as such in the Order Form or, if no date is specified, the date on which the Company commences provision of the Security Monitoring and Consultancy Services to the Customer.

2.2 The Minimum Term for the Security Monitoring and Consultancy Services shall be as set out in the Order Form, or if no Minimum Term is specified, twelve (12) calendar months from and including the Commencement Date.

3 MANAGED SIEM

3.1 Where specified in the Order Form that the Company is providing Managed SIEM, the Company will:

3.1.1 provide Incident Management for any Incidents relating to the availability of the SIEM Platform;

3.1.2 provide Problem Management for any Problems relating to the availability of the SIEM Platform;

3.1.3 agree a Security Incident Response Matrix during any transition or implementation phase of this Contract or otherwise as soon as reasonably practicable following the Commencement Date;

3.1.4 use reasonable endeavours to triage "Critical" and "High" alerts raised by the SIEM Platform to determine whether they should be escalated as Security Incidents within thirty (30) minutes of such alerts being raised;

3.1.5 notify the Customer of Security Incidents identified in paragraph 3.1.4 as soon as reasonably practicable in accordance with the Security Incident Response Matrix agreed with the Customer;

3.1.6 investigate Security Incidents using the capability of the SIEM Platform subject to the reasonable use policy specified in paragraph 8;

3.1.7 use reasonable endeavours to provide a Recommendation Report to the Customer for Security Incidents within the target timescales set out in the table below:

Severity	Target Timescale
Critical	Within 60 minutes
High	Within four (4) hours
Medium	Within twenty-four (24) hours
Informational	No timescales

3.1.8 generate and provide to the Customer regular reports as available as standard from the SIEM Platform at the frequency set out in the Order Form or, if no frequency is specified, on a monthly basis; and

3.1.9 host a call with the Customer and an appropriately skilled specialist to review and make recommendations relating to the reports provided in paragraph 3.1.8 at the frequency set out in the Order Form or, if no frequency is specified, on a monthly basis.

3.2 Where specified in the Order Form that the Company is providing "Purple Team Exercise", the Company will:

3.2.1 complete a simulated cyber attack on the Customer Environment to test the efficacy of the SIEM Platform on an annual basis unless otherwise specified in the Order Form; and

3.2.2 make changes relating to the configuration of the SIEM Platform to address the results of the activity specified in paragraph 3.2.1.

3.3 Where specified in the Order Form that the Company is providing "Threat Modelling Revalidation", the Company will update an existing Threat Model, if available, to reflect changes to the Customer Environment since its most recent update and will do so on an annual basis unless otherwise specified in the Order Form.

4 VULNERABILITY MANAGEMENT

4.1 Where specified in the Order Form that the Company is providing Vulnerability Management, the Company will:

4.1.1 provide access to the Service Desk to act as a point of contact for handling Service Requests and Incidents in relation to Vulnerability Management;

4.1.2 provide Incident Management for any Incidents relating to the Vulnerability Platform;

4.1.3 provide Problem Management for any Problems relating to the Vulnerability Platform;

4.1.4 complete Change requests relating to the configuration of the Vulnerability Platform, following the Service Request and Change Management processes;

4.1.5 notify the Customer when an update to a Vulnerability Scanner is required and provide reasonable information to enable the Customer to apply the update;

4.1.6 notify the Customer where reasonably possible ahead of the expiry of relevant licences for the Vulnerability Platform;

4.1.7 apply licence keys to the Vulnerability Platform under the governance of Change Management, where supplied by the Customer;

4.1.8 as soon as reasonably practicable, notify the Customer of vulnerabilities identified by the platform as "Critical" which are likely to impact the Customer; and

4.1.9 generate and provide to the Customer regular reports as available as standard from the Vulnerability Platform relating to the Customer Environment at the frequency set out in the Order Form or, if no frequency is specified, on a monthly basis.

4.2 Where specified in the Order Form that the Company is providing "Hosted Security Console", the Company will:

4.2.1 host a virtual console to be used by the Company for the management of the Vulnerability Platform; and

4.2.2 assign appropriate resources to the virtual console for the quantity of Assets specified in the Order Form.

5 VULNERABILITY MANAGEMENT AS A SERVICE (VMAAS)

5.1 Where specified in the Order Form that the Company is providing a "Vulnerability Scan", the Company will:

5.1.1 use the VMaaS Cloud Services to perform a Vulnerability Scan of an agreed range of IP addresses within the Customer Environment at the frequency set out in the Order Form or, if no frequency is specified, on a monthly basis; and

5.1.2 provide to the Customer via email a set of reports as defined by the Company, to include assessment results, high severity vulnerabilities, and vulnerability trend information, returned from each Vulnerability Scan.

5.2 Where specified in the Order Form that the Company is providing a "Perimeter Scan", the Company will:

5.2.1 use the VMaaS Cloud Services to perform a scan of the internet-facing devices within the Customer Environment at the frequency set out in the Order Form or, if no frequency is specified, on a monthly basis; and

5.2.2 provide a report to the Customer via email detailing any detected vulnerabilities, expiring or expired certificates, and any detected new hosts, ports, services or software in that period. No report will be sent if the scan does not discover any new events.

5.3 Where specified in the Order Form that the Company is providing a "Web Application Scan", the Company will:

5.3.1 for the number of applications and/or APIs specified in the Order From, create with the Customer a bespoke policy for each application or API to be scanned;

5.3.2 use the VMaaS Cloud Services to perform a scan on each application at the frequency set out in the Order Form or, if no frequency is specified, on a monthly basis; and

5.3.3 provide the results of the scan to the Customer upon completion of the scan.

5.4 Where specified in the Order Form that the Company is providing a "Review Call", the Company will:

5.4.1 host a call with the Customer and an appropriately skilled engineer to review and make recommendations relating to the reports provided in paragraphs 5.1, 5.2, and 5.3 above; and

5.4.2 host the call on a monthly or quarterly basis as specified in the Order Form.

6 PCI DSS ASV SCANNING

6.1 Where specified in the Order Form that the Company is providing "PCI DSS ASV Scanning", the Company will:

6.1.1 use the VMaaS Cloud Services to perform a quarterly Vulnerability Scan of an agreed range of IP addresses within the Customer Environment, not to exceed the maximum volume of IP addresses specified in the Order Form;

6.1.2 at the request of the Customer, use the VMaaS Cloud Services to perform additional ad-hoc Vulnerability Scans of an agreed range of IP addresses within the Customer Environment, not to exceed the maximum volume of IP addresses or scans specified in the Order Form;

6.1.3 at the request of the Customer, use the VMaaS Cloud Services to repeat a quarterly Vulnerability Scan of an agreed range of IP addresses within the Customer Environment, not to exceed the maximum volume of IP addresses or re-scans specified in the Order Form; and

6.1.4 provide remote support as specified in the Order Form:

(a) to assist with the understanding of any issues that result in a Vulnerability Scan that fails PCI DSS compliance and provide guidance in relation to appropriate remediation actions;

(b) where a Vulnerability Scan results in a 'false positive' failure, assist with the preparation of supporting evidence for the removal of such failure from a subsequent Vulnerability Scan; and

(c) use reasonable endeavours to answer any related PCI DSS questions.

7 SECURITY AWARENESS AND TRAINING SERVICES

7.1 Where specified in the Order Form that the Company is providing "Security Awareness and Training Services", the Company will

7.1.1 provide security and awareness training to the End Users as specified in the Order Form, in order to help identify potential risks and possible exposure to Cyber Threats and/or Malicious Content; and

7.1.2 from time to time at the Company's discretion, offer training and advice based on current best practice subject to clause 8.3.1.

7.2 As part of the Security Awareness and Training Services, the Customer will obtain appropriate prior approval and provide the Company with the authority to launch attacks on the Customer Environment, such as phishing, spear or whaling attacks, which will be randomly generated to target any End Users. It is the Customer's responsibility to inform the Company in advance with reasonable notice should there be any exceptions made as to End Users who should not be targeted.

7.3 The results from the Security Awareness and Training Services provided are for the Customer's own internal business purposes and neither party will disclose the results to any third party without the prior written consent of the other.

8 CUSTOMER OBLIGATIONS AND ACKNOWLEDGEMENTS

8.1 The Customer shall;

8.1.1 obtain all licences required for the Platform unless otherwise provided by the Company;

8.1.2 provide reasonable on-site remote hands assistance to assist with troubleshooting and diagnosing any issues;

8.1.3 ensure that the Customer Environment is correctly configured to provide access to the Platform and/or the VMaaS Cloud Services at all times;

8.1.4 not modify (or permit any third party to modify) the configuration of the Platform without the prior written consent of the Company;

8.1.5 be responsible for any third-party services or infrastructure it provides to enable the provision of Security Monitoring and Consultancy Services;

8.1.6 maintain subscriptions to Vendor specific licenses for the duration of the Contract in respect of the Platform;

8.1.7 be responsible for deployment of the Application to devices;

8.1.8 ensure that the Company is named as an authorised representative of the Customer where required on any third-party support and/or license agreements;

8.1.9 provide secure connectivity from the Company's management systems to the Customer Environment which is required to enable remote troubleshooting by the Company; and

8.1.10 inform the Company of any changes to the Customer Environment which may affect the provision of Security Monitoring and Consultancy Services including but not limited to the removal or addition of Log Sources and/or Assets.

8.2 The obligations set out in paragraph 8.1 shall apply to the Security Monitoring and Consultancy Services and the Company shall have no liability for any failure to provide the Security Monitoring and Consultancy Services under these Specific Conditions (including failing to meet any Service Level), or to pay any Service Credit (if applicable), to the extent caused by the Customer's failure to meet any of the obligations set out in paragraph 8.1.

8.3 The Customer acknowledges and agrees that:

8.3.1 the provision of the Security Monitoring and Consultancy Services, including the use of third-party services, does not provide a guarantee against Cyber Threats or Malicious Content, or a guarantee that the Customer Environment is free from every form of attack, flaw, or security weakness;

8.3.2 as part of the provision of the Security Monitoring and Consultancy Services, the Customer may be required to agree to third party licensing terms;

8.3.3 the VMaaS Cloud Services are owned by the Vendor and the Customer will not receive any license or right to use the VMaaS Cloud Services;

8.3.4 the VMaaS Cloud Services are provided by the Vendor "AS IS" and both the Company and the Vendor disclaim all express or implied warranties regarding the VMaaS Cloud Services;

8.3.5 the Vendor shall have no liability for either direct or consequential damages to the Customer; and

8.3.6 the Company reserves the right to change the VMaaS Cloud Services vendor at any time.

9 EXCLUSIONS

9.1 The following are excluded from the Security Monitoring and Consultancy Services provided under these Specific Conditions:

9.1.1 the provision and associated cost of any software licenses or renewals;

9.1.2 the provision or installation of hardware, software, licensing and/or security certificates that are required to meet the pre-requisites for any code upgrades or deployment methodologies released by the Vendor;

9.1.3 management of third-party support providers. The Company will on request pass relevant information in relation to the Platform to third party providers but will not manage that third party's performance of its obligations;

9.1.4 monitoring or configuration of any part of the Customer Environment;

9.1.5 all remediation actions including but not limited to forensic investigation of the Customer Environment or the backup and restoration of affected devices;

9.1.6 the support, configuration or management of any Platform functionality either not described in these Specific Conditions, not identified as included on the Order Form or identified as excluded on the Order Form;

9.1.7 where licenses or certificates are to be provided by the Customer to the Company for implementation, it is the responsibility of the Customer to provide such licenses or certificates in a timely manner for implementation prior to the expiry of the current license or certificate;

9.1.8 any liability for cyber incidents affecting the Customer, irrespective of whether the incident was detected by the SIEM Platform, Vulnerability Platform, VMaaS Cloud Services or Security Monitoring and Consultancy Services; and

9.1.9 any capability or service, including reporting, will only be provided to the extent feasible by the Platform and where the associated licenses have been purchased, and/or relevant configuration or deployment methodology has been applied.

10 CHARGES

10.1 The Charges for the Security Monitoring and Consultancy Services will be as identified in the Order Form.

10.2 The Charges will be invoiced annually in advance or as otherwise stated in the Order Form, with the first invoice issued by the Company on or around the Commencement Date and annually thereafter.

10.3 The Charges agreed relate to the existing or proposed Customer Environment, SIEM Platform and/or Vulnerability Platform as known to the Company as at the Effective Date. If these elements change the Company may take reasonable steps to address this including but not limited to those specified in paragraph 11.2. Changes may include:

10.3.1 changes to the Customer Environment;

10.3.2 changes to the information available to the Company about the Customer Environment;

10.3.3 changes to the level of Security Monitoring and Consultancy Services required;

10.3.4 changes to the SIEM Platform elements enabled or deployed; and/or

10.3.5 changes to the Vulnerability Platform elements enabled or deployed.

11 REASONABLE USE

11.1 All Security Monitoring and Consultancy Services are provided on a reasonable use basis, as determined by the Company.

11.2 If, using its reasonable judgement, the Company considers that the use of the Security Monitoring and Consultancy Services by the Customer has consistently or notably exceeded any volumes or parameters stated in the Order Form or typical usage by other customers, or that an individual Service Request made by the Customer is not reasonable in nature, the Company may take reasonable steps to address the usage pattern or Service Request. Such steps may include:

11.2.1 remedial work to address the root cause of the issues that are causing overuse of the Security Monitoring and Consultancy Services, such work being chargeable by the Company on a time and materials basis;

11.2.2 revising recurring charges or imposing additional time and materials charges in consideration of the overuse / request;

11.2.3 limiting the Customer's use of the Security Monitoring and Consultancy Services in line with typical customer use; and/or

11.2.4 implementation of a fair use policy relating to the Security Monitoring and Consultancy Services or to a particular element of the Security Monitoring and Consultancy Services.

11.3 Where the Company finds that the cost of delivering the Security Monitoring and Consultancy Services is greater than one hundred and twenty-five percent (125%) of the on-going managed service charges in relation to a particular Security Monitoring and Consultancy Service as detailed in the Order Form within any three (3) month period, the Company reserves the right to review and change the agreed commercial terms and/or impose relevant restrictions as identified under paragraph 11. 2

12 SERVICE LEVELS

12.1 The Company will provide the management of Incidents in accordance with the Specific Conditions X3 – Standard Operational Services.

12.2 The Company will supply the Request Fulfilment in accordance with the Specific Conditions X3 – Standard Operational Services.