SPECIFIC CONDITIONS N6 – SECURITY OPERATIONS CENTRE SERVICES

These Specific Conditions govern the Security Operations Centre 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 Operations Centre 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:

"Asset"	means a server or End User device within the Customer Environment;
"Collector"	means a virtual or physical machine that is responsible for collecting Logs from Log Sources within the Customer Environment and forwarding them to the SIEM Platform;
"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;
"Customer Environment"	means the Customer Assets, applications, and devices which the SIEM Platform and/or EDR Platform will monitor and report on, as agreed in writing by the parties;
"EDR Application"	means any security application or agent required for specific functionality of the EDR Platform, to be installed on an Asset;
"EDR As A Service"	means the Services provided to the Customer by the Company as detailed in paragraph 4 of these Specific Conditions, if detailed in the Order Form;
"EDR Platform"	means the cloud hosted endpoint detection and response platform that is used by the Company in the provision of EDR As A Service and made available online by the Vendor, including any offline components and data;
"Log Source"	means an Asset, application or device within the Customer Environment that has been configured to send Logs to the Collector;
"Logs"	means a record of security information created by a device within the Customer Environment and analysed by the SIEM Platform and/or EDR Platform;
"Malicious Content"	means any type of malware, ransomware, spyware, adware, scareware, virus, worm, Trojan horse, or other computer program or software code used to disrupt computer operation, gather sensitive information, or gain access to private computer systems;
"Recommendation Report"	means a report provided to the Customer following an identified Security Incident comprising overview, severity level, potential impact, affected devices, recommended action and further reading;
"Security Incident"	means a cyber security incident relating to the Customer Environment as detected by the SIEM Platform and/or EDR 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 Operations Centre Services"	means collectively the services provided to the Customer by the Company as described in these Specific Conditions including SIEM As A Service and/or EDR As A Service, where applicable;
"SIEM Application"	means any security application or agent required for specific functionality of the SIEM Platform, to be installed on an Asset;
"SIEM As A Service"	means the Services provided to the Customer by the Company as detailed in paragraph 3 of these Specific Conditions, if detailed in the Order Form;
"SIEM Platform"	means the cloud hosted security information and event management platform that is used by the Company in the provision of SIEM As A Service and made available online by the Vendor, including any offline components and data;
"Threat Model"	means a report of the Customer Environment which identifies the Assets, applications and devices most vulnerable to a Security Incident; and
"Virus Definitions"	means the virus definitions provided by the Vendor as updated from time to time.

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 Operations Centre 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 Operations Centre Services to the Customer.

2.2 The Minimum Term for the Security Operations Centre 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 SIEM AS A SERVICE

3.1 Where specified in the Order Form that the Company is providing SIEM As A Service, the Company will:

3.1.1 use the SIEM Platform to collect and analyse Logs sent to it by the Customer Environment;

3.1.2 make available a Collector to be deployed by the Customer in the Customer Environment;

3.1.3 make available a SIEM Application to be deployed by the Customer on Assets in the Customer Environment;

3.1.4 provide Incident Management for any Incidents relating to the availability of the SIEM Platform and/or the Security Operations Centre Services;

3.1.5 provide Problem Management for any Problems relating to the availability of the SIEM Platform and/or the Security Operations Centre Services;

3.1.6 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;

3.1.7 use reasonable endeavours to triage 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;

3.1.8 notify the Customer of Security Incidents identified in paragraph 3.1.7 as soon as reasonably practicable in accordance with the Security Incident Response Matrix agreed with the Customer;

3.1.9 investigate Security Incidents using the capability of the SIEM Platform;

3.1.10 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

3.1.11 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

3.1.12 host a call with the Customer and an appropriately skilled specialist to review and make recommendations relating to the reports provided in paragraph 3.1.11 at the frequency set out in the Order Form or, if no frequency is specified, on a monthly basis.

3.2 Where specified on the Order Form that the Company is providing "Purple Team Testing", 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 on 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 on 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 EDR AS A SERVICE

4.1 Where specified in the Order Form that the Company is providing EDR As A Service, the Company will:

4.1.1 make available an EDR Application to be deployed by the Customer on Assets in the Customer Environment;

4.1.2 use the EDR Platform to continuously monitor the Assets to detect and mitigate Malicious Content and/or Cyber Threats;

4.1.3 within thirty (30) minutes of an alert being raised by the EDR Platform, use reasonable endeavours to investigate such alerts and:

(a) confirm that any alert of Malicious Content and/or a Cyber Threat that has been prevented or blocked through any automated investigation and remediation by the EDR Platform requires no further action;

(b) escalate any alert that was not able to be automatically remediated by the EDR Platform or requires further action to a Security Incident and notify the Customer as soon as reasonably practicable in accordance with the Security Incident Response Matrix agreed with the Customer; and

(c) within the target timescales set out in the table below:

(i) using the capability of the EDR Platform, investigate and take appropriate and reasonable measures to remediate the Security Incident; or

(ii) where a Security Incident cannot be remediated using the capabilities of the EDR Platform, notify the Customer of recommended actions.

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

4.1.4 use the EDR Platform to manage updates to the Virus Definitions on the Assets, providing notification to the Customer of any non-compliant Assets;

4.1.5 upon receipt of a Service Request from the Customer to restore a file quarantined by the EDR Platform or to configure an exclusion rule:

(a) review the Service Request to assess the possible impact and/or risk to the Customer Environment;

(b) based on that review and assessment, provide a recommendation to the Customer as to whether the Service Request should be completed; and

(c) complete the Service Request upon receipt of written approval to do so by the Customer, such approval to be considered acceptance by the Customer of any associated risk advised by the Company.

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

4.1.7 host a call of no more than one (1) hour duration with the Customer and an appropriately skilled specialist to review and make recommendations relating to the reports provided in paragraph 4.1.63.1.11 at the frequency set out in the Order Form or, if no frequency is specified, on a quarterly basis;

4.1.8 provide Incident Management for any Incidents relating to the availability of the EDR Platform and/or the Security Operations Centre Services; and

4.1.9 provide Problem Management for any Problems relating to the availability of the EDR Platform and/or the Security Operations Centre Services;

5 CUSTOMER OBLIGATIONS AND ACKNOWLEDGEMENTS

5.1 The Customer shall;

5.1.1 deploy and manage any required EDR Applications, Collectors or SIEM Applications within the Customer Environment on appropriate virtual machines, hardware and/or operating systems as instructed by the Company;

5.1.2 where applicable, configure all Log Sources to send their Logs to Collectors deployed in the Customer Environment;

5.1.3 be responsible for the deployment of the SIEM Application and/or the EDR Application to Assets;

5.1.4 make any required configuration changes to allow SIEM Applications to collect data on the Assets and to send their Logs to Collectors or the SIEM Platform;

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

5.1.6 ensure that the Customer Environment is correctly configured to provide access to the SIEM Platform and/or the EDR Platform at all times;

5.1.7 be responsible for any third-party services or infrastructure it provides to enable the provision of the Security Operations Centre Services;

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

5.1.9 inform the Company of any changes to the Customer Environment which may affect the provision of the Security Operations Centre Services including but not limited to the removal or addition of Log Sources;

5.1.10 not: (i) upload or otherwise transmit, display, or distribute any Customer Input Materials to the Security Operations Centre Services that infringe any trademark, trade secret, copyright, or other proprietary or intellectual property rights of any person; (ii) upload or otherwise transmit to the Security Operations Centre Services any material that contains software viruses or any other computer code, files, or programs designed to interrupt, destroy, or limit the functionality of any computer software or hardware or telecommunications equipment; or (iii) interfere with or disrupt the Security Operations Centre Services; and

5.1.11 except as may be expressly permitted by Relevant Laws not: (i) merge the Security Operations Centre Services into another program; (ii) circumvent or disable any security or technological features or measures in the Security Operations Centre Services; nor (iii) access the Security Operations Centre Services in order to build a competitive product or service, for competitive analysis, or to copy any ideas, features, functions, or graphics of the Security Operations Centre Services.

5.2 The Customer covenants to the Company that it is the sole owner of, or has legal authority to grant access to, the Customer Environment to be accessed by the Company and/or the Vendor in providing the Security Operations Centre Services. This includes authority to remotely scan, monitor and/or test related systems and all other authority to access systems given by the Customer to the Company through allocated access or account activation.

5.3 The SIEM Platform's orchestration and automation functionality is not designed, intended, or licensed for use in hazardous environments or other applications where a malfunction could cause property damage or personal injury, and the Company specifically disclaims any liability in connection with any such use. The Customer assumes all risks in using third-party products or services in connection with the SIEM Platform.

5.4 In the event that the Customer is using the SIEM Platform to engage in illegal activity, and/or the Customer's use of the Service is causing immediate, material and ongoing harm to others, the Customer agrees that the Company may immediately cease to provide SIEM As A Service to the Customer.

5.5 The Company shall have no liability for any failure to provide the Security Operations Centre 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 5.

5.6 The Customer acknowledges and agrees that:

5.6.1 the SIEM Platform and/or EDR Platform are owned by the respective Vendors and the Customer is permitted to access the SIEM Platform and/or EDR Platform provided that the Customer complies with the Contract;

5.6.2 the SIEM Platform and/or EDR Platform are provided by the respective Vendors "AS IS" and both the Company and the Vendor disclaim all express or implied warranties regarding the SIEM Platform and/or the EDR Platform;

5.6.3 the Vendor shall have no liability to the Customer; and

5.6.4 the Company reserves the right to change the SIEM Platform and/or EDR Platform Vendor on reasonable notice to the Customer and the Customer shall provide reasonable assistance to the Company in this regard.

6 EXCLUSIONS

6.1 The following are excluded from the Security Operations Centre Services:

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

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

6.1.3 monitoring or configuration of any part of the Customer Environment unless specifically stated otherwise in these Specific Conditions or the Order Form;

6.1.4 all remediation actions including but not limited to forensic investigation of the Customer Environment, incident response activities, or the backup and restoration of affected devices, unless specifically stated otherwise in these Specific Conditions or the Order Form;

6.1.5 any responsibility for loss or damage to Logs which are stored in the SIEM Platform and/or the EDR Platform;

6.1.6 the support, configuration or management of any SIEM Platform and/or EDR Platform functionality not described in these Specific Conditions, not identified as included on the Order Form and/or identified as excluded on the Order Form;

6.1.7 any liability for cyber incidents affecting the Customer, irrespective of whether the incident was detected by the Security Operations Centre Services; and/or

6.1.8 any capability or service, including reporting, will only be provided to the extent feasible by the SIEM Platform and/or EDR Platform.

6.2 From time to time the SIEM Platform and/or EDR Platform may be inaccessible or inoperable due to various reasons, including but not limited to equipment malfunctions and periodic maintenance procedures or repairs which the Vendor may undertake from time to time and the Company will have no liability for such inaccessibility or inoperability.

6.3 The Company is not responsible for any data lost or corrupted or rendered inaccessible from the Customer Environment or otherwise as a result of any Security Incident, or caused by misuse of any system or application hosted in or connected to the Customer Environment by End Users or breach by End Users of any security policy.

7 CHARGES

7.1 The Charges for the Security Operations Centre Services will be as identified in the Order Form.

7.2 The Charges will be invoiced quarterly 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 quarterly thereafter.

7.3 The Charges agreed relate to the existing or proposed Customer Environment, SIEM Platform, and/or EDR 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 paragraphs 8.2 and/or 8.3. Changes may include:

7.3.1 changes to the Customer Environment;

7.3.2 changes to the information available to the Company about the Customer Environment; and/or

7.3.3 changes to the SIEM Platform and/or EDR Platform elements enabled or deployed.

8 REASONABLE USE POLICY

8.1 All Security Operations Centre Services are provided on a reasonable use basis, as determined by the Company.

8.2 If the volume of data sent to the SIEM Platform by Log Sources consistently exceeds on average 0.8GB per Asset per month, the Company may take reasonable steps to address the usage. Such steps may include but are not limited to:

8.2.1 making changes related to the configuration of the SIEM Platform to reduce the volume of data ingested by the SIEM Platform;

8.2.2 requesting that the Customer makes configuration changes to Log Sources to reduce the volume of data sent to Collectors and/or the SIEM Platform; and/or

8.2.3 revising recurring charges or imposing one-off charges in consideration of the overuse.

8.3 If, using its reasonable judgement, the Company considers that the use of the Security Operations Centre Services by the Customer has consistently or notably exceeded 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:

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

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

8.3.3 limiting the Customer's use of the Security Operations Centre Services in line with typical customer use; and/or

8.3.4 changing a particular element of the Security Operations Centre Services.

8.4 Where the Company finds that the cost of delivering the Security Operations Centre Services is greater than one hundred and twenty-five percent (125%) of the Charges in relation to the Security Operations Centre Services 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 8.3.

9 SERVICE LEVELS AND LIMITED WARRANTY

9.1 The Company will provide Incident Management, Problem Management and Change Management in accordance with the applicable Service Levels set out in Specific Conditions X3 – Standard Operational Services.