CALL-OFF SCHEDULE: PRODUCT SPECIFIC TERMS – TMC3 MSSP – MANAGED SOC

1. INTERPRETATION AND RELATIONSHIP TO CCS GENERAL TERMS

1.1. This Schedule sets out the Product Specific Terms for the provision of TMC3 MSSP – Managed SOC. It is incorporated into the Call-Off Contract formed between the Buyer and the Supplier.

1.2. In this Schedule, the following terms shall be interpreted as follows to align with the **CCS General Terms**:

- **"Buyer"** replaces "Customer".
- **"Order Form"** replaces "Ordering Document".
- **"Start Date"** replaces "Services Start Date" or "Effective Date".
- **"Contract Period"** replaces "Term".

1.3. Unless defined in this Schedule, capitalised terms have the meaning given in the CCS General Terms or Joint Schedule 1 (Definitions). In the event of a conflict between this Schedule and the CCS General Terms, the CCS General Terms shall prevail unless Special Terms in the Order Form state otherwise.

2. SUPPLIER OBLIGATIONS

As applicable based on the Supported Sources, the Supplier shall:

2.1. Fine Tuning Phase (a) From the Start Date for the Fine Tuning Phase the Service Level Agreement does not apply while the Security Alerts are fine tuned; (b) Work with the Buyer to reduce the number of False Positives and critical alerts during the Fine Tuning Phase.

2.2. Reactive Support (a) Respond to Security Incidents raised by a Buyer Named Contact in accordance with the Service Level Agreement; (b) Reclassify the priority of a Security Incident raised by the Buyer where incorrectly prioritised by the Buyer; and (c) Track and report Security Incidents raised by the Buyer activities in the Supplier Support Portal.

2.3. 24/7 Managed Detection & Response (a) Continuously detect, investigate and provide context around Security Threats; (b) Monitor the Supported Sources 24/7 to detect and identify Security Threats which may be raised as Security Alerts; (c) Respond to Security Threats and Security Alerts with Recommended Remediation Guidance; and (d) Notify the Buyer within the relevant Response Time SLA of an on-going Security Incident.

2.4. Google SecOps Platform Management (a) Proactively support Google SecOps SIEM data source integrations, onboarding and fine-tuning of the platform; and (b) Design, implement, integrate and fine-tune the Google SecOps SOAR automation playbooks for new and existing detection use-cases.

2.5. Threat Modelling and Use Case Designing (a) Create and share threat-centric use cases using the latest threat intelligence across the Supported Services.

2.6. Threat Intelligence Enrichment (a) Proactively enhance managed detection and response capabilities by enriching ingested data with enterprise-grade and open-source threat intelligence sources specific to the Buyer's industry; and (b) Develop custom threat hunting rules by analysing complex, non-atomic threat intelligence data to uncover new and sophisticated threats that may bypass predefined detection mechanisms.

2.7. Compliance Scanning (a) Proactively scan the Buyer Public Cloud environments against Centre for Internet Security ("CIS") benchmarks; and (b) Share a monthly report defining CIS benchmark findings.

2.8. KPIs & Reporting (a) Provide monthly reporting that summarise KPI performance, trends, and key findings across relevant Key Metrics, as agreed with the Buyer from time to time.

2.9. EDR Operations (a) Proactively monitor and fine tune the Buyer's Endpoint Protection Platform ("EPP") or Endpoint Detection and Response Solution ("EDR"), ensuring the tools are updated to deliver operational value; and (b) Take action in the Buyer EDR / EPP once approval has been granted by the Buyer.

3. BUYER OBLIGATIONS

The Buyer shall:

3.1. Have an active Google SecOps SOAR and SIEM platform licence ("Google SecOps Platform") in place for the Supported Sources, either purchased via the Supplier or purchased elsewhere;

3.2. Deploy the necessary Agents and Configurations to enable the Supplier to onboard SIEM data sources;

3.3. Provide the necessary level of delegated access to the Buyer Google SecOps Platform to the Supplier;

3.4. Manage and operate the Buyer EDR / EPP service, if applicable;

3.5. Provide the necessary level of delegated access to the Buyer EDR/EPP service to the Supplier, if applicable;

3.6. Remedy any Security Threats and Security Incidents discovered during the onboarding and Fine Tuning Phase within 1 month of the Fine Tuning Phase concluding. Any Security Threats and Security Incidents that remain unaddressed after 1 month will be muted by the Supplier and will not be covered under the Managed Security Services; and

3.7. Remedy all Security Threats and Security Incidents using the Recommended Remediation Guidance provided by the Supplier.

4. DEFINITIONS

The following definitions apply in these Product Specific Terms:

Agents and Configurations: means including but not limited to installing new agents, creating API keys or credentials and altering firewall & network configurations to facilitate log collection.

Buyer Named Contact: means a Buyer appointed individual authorised to raise Security Incidents in line with the SLA.

Change Request: means a request for consultancy, or to make an impactful change to the Supported Sources, that requires risk analysis, planned outage, further approval and or planning / coordination between the Buyer and Supplier.

False Positive or FP: means a Security Alert that is triggered based on a Security Threat that is benign.

Fine Tuning Phase: means as defined in the Order Form.

Google SecOps SIEM: means a cloud native security information and event management ("SIEM") solution, enables users to collect and analyse security telemetry from across their enterprise to power detection, investigation, and remediation of threats.

Google SecOps SOAR: means a cloud native security, orchestration, automation and response ("SOAR") solution, empowers security teams to respond to cyber threats in minutes. SecOps SOAR fuses a unique threat-centric approach, powerful playbook automation, and context-rich investigation.

Key Metrics: means as set out in Schedule 1.

MDR: means managed detection and response.

Protocol-Specific Logs: means including but not limited to: DNS, HTTP, SMB, FTP.

Public Attack Surface: means the points of entry and vulnerabilities an attacker can exploit to infiltrate a network or a system from the internet.

Public Cloud: means Google Cloud Platform ("GCP"), Amazon Web Services ("AWS") and Microsoft Azure ("Azure").

Recommended Remediation Guidance: means the steps required by the Buyer to resolve a Security Threat or Security Incident.

SecOps Threat Intelligence Platform: means a cloud native insight platform providing visibility into the global threat landscape.

Security Alert: means an automated or manual notification made to make the Supplier or the Buyer aware of a Security Threat or Security Incident that poses an active risk to the Buyer’s environment. Security Alerts classified as informational or informative are out of scope unless correlated with additional alerts of higher severities.

Security Incident: means a Security Threat or group of Security Threats that pose an active risk to the Buyer’s environment and requires active management until resolution.

Security Threat: means a notification of a log event that has the potential to become a Security Incident if it is not addressed.

Service Level Agreement or SLA: means as set out in Paragraph 6 below.

Service Request: means a request to make a low impact change to the Supported Sources, that does not require any risk analysis or further approval.

Supported Sources: means as defined in the Order Form.

6. SERVICE LEVEL AGREEMENT (SLA)

6.1. The Supplier shall provide support in accordance with the table below:

Priority Level	Description	Response Time	Availability	Available Support Channels*
P1	Immediate risk including suspected or high probability of system compromise	30 minutes	24/7	Phone outside of Business Hours.Support Portal or Email during Business Hours.
P2	High risk of increased attack activity including high priority events that may require further investigation by the Buyer	2 Hours	Business Hours	Support Portal, Email or Phone during Business Hours
P3	Low risk indicates the need for increased vigilance in monitoring and will be used to keep Buyer informed about potentially hostile activity.	1 Business Day	Business Hours	Support Portal, Email or Phone during Business Hours
P4	Change Requests and Service Requests	2 Business Days	Business Hours	Support Portal or Email

6.2. **Available Support Channels**:

Channel	Contact Details
Support Portal	https://support.qodea.com
Email	mdr@qodea.com

Phone 01793 391477

SCHEDULE 1 - KEY METRICS

KPI	Definition
Total Number of Security Alerts	The total number of Security Alerts
Mean time to Acknowledge (MTTA)	The average amount of time it takes for the Supplier to acknowledge a Security Alert before investigation occurs.
Mean time to Resolution (MTTR)	The average time it takes to completely resolve a Security Incident once it has been detected. This includes root cause analysis, deployment of configuration changes or fixes and any recovery actions required.
Alerts / Use Cases	The total number of alerts in relation to the respective SIEM use cases provided by the Supplier
Alerts / SOAR Playbooks	The total number of alerts in relation to the respective SOAR playbooks provided by the Supplier
Event Quality	The number of resources with parsing-errors
Resolved Alerts	The total number of resolved alerts
True Positives	The number of True Positive alerts
False Positives	The number of False Positive alerts
Compliance Audit Results	The results of compliance audits, including the number of non-compliant items identified, number of assets with incompliances, number of assets violating PCI, GDPR etc. the severity of the non compliance, and the time to remediate non-compliant items
Severity Distribution	The distribution of vulnerabilities by severity level, such as critical, high, medium, and low
Resolution Time Incident	The amount of time it takes the incident response team to get from investigation to recovery