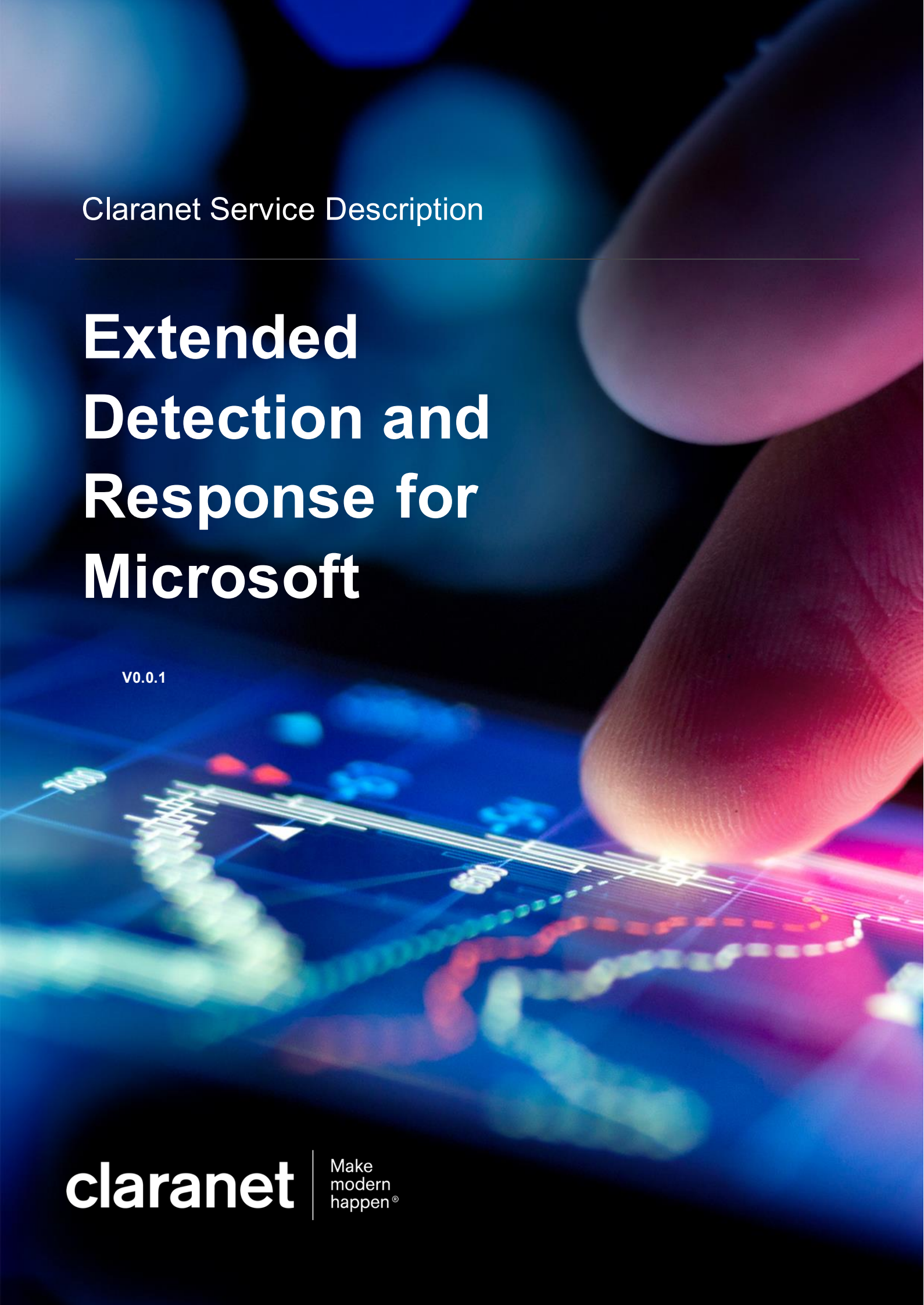
Claranet Service Description

Extended Detection and Response for Microsoft

V0.0.1



claranet | Make modern happen®

Contents

1. Introduction

This Service Description describes the service Claranet provides and details the Customer's responsibilities in relation to this Service. The Service Description forms part of the Agreement between the Parties and should be read in conjunction with the terms of the Claranet Master Services Agreement ("MSA") set out at www.claranet.co.uk/legal or as otherwise agreed by the Parties and the Parties agree to be bound by such terms. Unless otherwise specified, all terms used within this document are in accordance with the terms to be found in the MSA.

Claranet provides the following services as part of its Extended Detection and Response for Microsoft ("XDR/Service"). The Service components and features are set out below along with the related responsibilities for that Service component/feature.

2. Scope of Service Description

The Customer agrees that any services, activities, and deliverables not expressly set out within this Service Description shall be out of scope for the Service. Any components which are described as optional or additional in this Service Description will be chargeable at additional cost and will need to be purchased by the Customer and an Order Form or Statement of Works will need to be signed by the Customer.

Notwithstanding the foregoing, in the event Claranet completes additional services, activities and/or deliverables upon the request or at the direction of the Customer, Customer shall be responsible for the payment of all Fees and expenses associated therewith, whether or not an Order Form or Change Request has been executed.

3. Service Overview

The Service provides prevention techniques and response actions to confirmed threats, and in-depth investigation and remediation to suspicious activity, protecting the Customer's network and endpoints before the attack evolves.

Analyst driven; Claranet provides rapid investigation of security alerts generated by end points on the Customer's network. The Customer receives valuable information and or remediation on a 24x7x365 basis from skilled technical support.

4. Service Features

The Service supports the following features:

4.1 Standard Features

The following features are supported and included as standard:

Feature	Description
Claranet Online	The Claranet Online portal is the repository for Incident tickets and where the Customer can raise queries, submit change requests, access monthly reports or respond to Incidents. The Customer will receive a notification from Claranet Online when an Incident ticket is generated.

Assisted Installation	The Security Operation Centre (SOC) Engineers will aid system administrators in deploying the agents onto the Customer's Endpoints, including API integrations, cloud environments and other infrastructure. Communications will be validated between the log source and Claranet Online. Claranet's engineers will also assist the Customer with onboarding one of each type of in scope log source - a process that will normally take 30 days. Tuning begins as soon as a log source is onboarded. Billing for onboarded log sources shall begin after 30 days. Where there is a delay to onboarding a log source that is outside of Claranet's control, such as a delay caused by the Customer or made on behalf of the Customer, Claranet will commence billing after 30 days and the Service will be considered as delivered. Thereon, Claranet will continue to work with the Customer to onboard and tune any remaining in scope log sources and features as documented on the Statement of Work ("SOW") and Asset Verification Form. Please note that a Project Manager will be assigned to the onboarding to ensure the success of the project.
Incident Detection	Event information, received from log sources on the Customer's infrastructure, are sent to Microsoft Sentinel. If the Events meet the criteria of a detection rule, an Incident ticket will be created which is then reviewed, analysed, and prioritised by Claranet's Security Analysts according to the Response matrix in Section 8.1.
Incident Notification	The Customer will receive Incident Notifications for Priority 1 to Priority 4. While the Customer does not receive a Notification of Priority 5 Incidents directly, the totals are displayed in the monthly reports. For more detail on the Notification levels, please see the Response Matrix in section 8.1.
Incident Management	SOC Analysts will make recommendations for remediation, root cause analysis based on log investigations, identifying the initial attack vector and provide remediation advice and techniques. This includes establishing or attending calls with the Customer, and with members of the Customer's team, to discuss the attack in more detail if required.
Threat Intelligence	Threat Intelligence uses open sources, which include publicly available information regarding Indicators of Compromise (IOCs) such as domains, IP addresses, file hashes etc., and closed sources such as UK Government, other Customer deployments, and working closely with other security business units within the Claranet group. This information is fed into the Microsoft Sentinel Instance and used by the SIEM to enrich Incident investigations.

	Claranet's SOC Analysts will review the Incidents and follow the notification path based on the priorities outlined in Section 8.
Threat Hunting	Threat hunting involves SOC Analysts performing proactive searches for potential breaches. These threat hunts search for IOCs based on Tactics, Techniques and Procedures (TTPs). Threat hunting for specific TTPs involves having a deep understanding of the MITRE ATT&CK® Matrix for Enterprise. SOC Analysts will develop hypotheses around how a threat actor may have accessed the Customer's environment and what activities were performed once inside. Hunting queries are then developed to manually search for evidence to support the hypotheses. Should anything be found within the Customer's environment, an Incident ticket will be raised.
Tuning	The purpose of tuning is to remove as many false positives as possible to ensure that Incident notifications remain relevant. Tuning will be performed continuously throughout the life of the Service. Claranet will proactively tune the Customer's detection rules to reduce false positives and increase coverage of the MITRE attack framework over the course of the Service.
Custom Detection Rules	The Customer will have the ability to request Custom Detection Rules that are specific to the Customer's environment. These can be requested via Claranet Online as part of the Change Management process.
Response Actions	Delivering the Service involves the investigation of, and potential initiation of Response Actions on the Customer's live systems on its current infrastructure. This may therefore have an impact on current workloads and environments. Scope of Response Actions will be discussed during onboarding meetings.
Platform Support (Monday to Friday (09:00hrs to 17:30hrs GMT)	SOC Engineers are available to support the operational components of the in-life Service, this includes assisting with onboarding new agents, decommissioning agents or troubleshooting issues with agents. Where the Engineering team cannot directly resolve an issue, they will escalate any platform issues to Microsoft on the Customer's behalf and work with Microsoft to resolve the issue.
Monthly Report	A Monthly Report will provide a summary of the Incidents discovered during the month, all P1 to P5 Incidents, and outcomes of threat hunting.
Quarterly Review	The SOM will conduct a Quarterly Service Review with the Customer every three months. In this meeting, both parties will discuss utilisation and usage

	thresholds, the Incidents processed during the period, breakdown of false positives and benign Events vs Incidents, SLA metrics that have been met and service improvement recommendations.
Log storage queries	Claranet will query the Customer's log data within its Microsoft Sentinel instance as part of an investigation. The following are included as standard within the Customer's Microsoft tenant: • Data is stored in the Defender tenant for 90 days as standard and will be visible in the Defender portal. • Microsoft Sentinel will house data for 90 days, with different options to extend this beyond but would be subject to additional cost payable by the Customer to Microsoft. • Data storage locations may also be requested based on geographic location, but by default, a UK data centre will be selected for any new Microsoft Sentinel deployment. • Advanced Hunting data is used for investigation and threat hunting is accessible for 90 days via Kusto Query Language (KQL). This can be extended indefinitely within the Customer's Microsoft tenant at additional cost payable from the Customer to Microsoft.

5. Service Operation

This Service shall be read in conjunction with the 'Claranet SOC Customer Handbook' (the "Handbook"), which shall be provided separately and provides a framework for Claranet's support for the Service solution provided by Claranet within this Service Description (the "Handbook"). This Handbook is intended to supplement this Service Description. In the event that this Service Description conflicts with the Handbook, the provisions of this Service Description will prevail to the extent of such conflict.

In the event the Customer or Claranet requires a change that impacts Service features, components and/or Fees, such changes must be captured in an Order Form and/or SOW. In the event that any other change is required that does not impact the foregoing or the Fees relating to the Service, then the parties may agree to such changes as an ongoing management activity of the Service.

6. Customer Responsibilities

The Customer, or any appointed third parties, acknowledge and agree to perform its responsibilities. Claranet's delivery, implementation and performance of the Service is dependent upon the timely and effective completion of the Customer's roles and responsibilities and/or as per Claranet's reasonable instructions. If the responsibilities as set out below are not met, and any Service Levels set out herein are impacted, Service Credits will not apply as a result:

Responsibility	Description
Provide a suitable primary contact for the length of the Service.	To ensure smooth delivery of the Service, the Customer must provide Claranet with a primary contact with the relevant knowledge and experience to provide all necessary assistance to Claranet pursuant to this Service Description and/or the SOW.
Access to key staff and stakeholders.	The Customer must provide key staff and stakeholders, both internal and external (where relevant), are available for engineer visits, meetings and/or workshops. This includes a designated Services contact as a decision-maker for a subset of operational issues pertaining to the Service, Claranet will only interface and provide updates to a designated point of contact regarding security incidents dependant on the Customer's nomination of the individual or group.
Provide a safe and suitable working environment.	Where Claranet employees are required to attend Customer and/or third-party premises, the Customer must ensure that Claranet employees are provided with a safe and suitable working environment.
Provide information required by Claranet.	The Customer shall provide any information requested in the format specified by Claranet within five (5) working days, unless agreed otherwise in writing.
Responding to project requests by Claranet.	The Customer shall respond to any project-related request made by Claranet within five (5) working days, unless agreed otherwise in writing.
Provide access, support and personnel	The Customer will provide the necessary access, support and relevant personnel to complete the Project.
Reasonable and timely cooperation	The Customer will provide reasonable and timely cooperation and follow instructions as required by Claranet.
Managing Customer-managed stakeholders	The Customer will be responsible for all communications to all key or relevant Customer-managed stakeholders regarding the Service for the project's duration, including any technical change and/or approval required by Claranet.
Notifications regarding maintenance	The Customer will inform Claranet of any scheduled maintenance or emergency maintenance within reasonable notice that will affect the Service's performance.
Changes to information	The Customer will ensure that technical details are kept up to date by submitting them to Claranet, Claranet will verify to confirm or update the relevant details, in accordance with the Service Operation.
ClaranetOnline	The Customer will not share user accounts or give these accounts to third parties. The failure to safeguard the Customer's individual logins could result in the loss of confidential data and this will not be the

	responsibility of Claranet. This behaviour can also lead to the disabling of accounts and the reduction of the number of allowed user licenses.
Microsoft Licensing	The Customer is responsible, unless agreed otherwise, for procuring and maintaining such licensing to ensure that Claranet can perform the Service, and that the Customer upholds its compliance to Microsoft licensing.
Security testing	Customer must inform Claranet of any planned penetration testing or other similar services that may impact this Service, and Claranet must approve any such instances. This is because these penetration tests and other services can overwhelm the Claranet SOC with alerts and need to be agreed before commencement. In the event Claranet are not made aware of this and approved the test in advance, the Service SLAs shall not apply and Claranet may charge a fee of up to 50% of the monthly Fees in the relevant month, as pre-agreed additional charges for the additional effort.
Adding additional log sources	Through the change process, the Customer will be able to add log sources to the Service during the contract period by making a request through the Claranet Online portal. Before Claranet can start monitoring all the Customer's Events on a newly requested log source, there are certain configurations that must be in place to ensure that the data store is receiving all of the relevant Event logs. Any additional log sources the Customer wishes to add will be evaluated, configured, and set up correctly. If the Customer does not notify the SOC Team, any additional log sources will not be monitored and will be considered out of scope. Any additional log sources will be recorded on the Customer's Asset Verification Form. Adding additional log sources may incur additional Managed Service Fees and will be determined through a scoping exercise. Additional Fees may be incurred and an Order Form will be provided for additional log sources above the original Data Tier as.

7. Pre-Requisites

Before Claranet can commence the Services, the Customer is required to complete the following pre-requisite activities to ensure that the Services can be delivered successfully. If such pre-requisite activities are not met by the Customer, then this may have adverse impact on the delivery of Services and may prevent Claranet from delivering on its obligation and/or require changes in a Change Request Form to remediate any impact.

Pre-requisite Activity

The Customer will provide access to the licensing and technical information managed by the Customer that is required for the delivery of the Service by Claranet.
The Customer will attend all the project planning and workshop(s) sessions to establish the scope of Service that it requires.
The Customer will provide all information requested in the format specified by Claranet within five (5) working days of request.
The Customer will provide a mechanism for the roll out of the agent across the Customer's network, such as, but not limited to, Intune.
The Customer will provide Claranet with a list of people to respond to the security incidents via the Claranet Online portal and be responsible for the incidents through to closure including a distribution email address to contact these people.
To enable the SOC Engineers and SOC Analysts to access the Microsoft Sentinel instance, workbooks, and automation rules located inside the Customer's Azure tenant resources, Claranet will utilise a service called Lighthouse. The Customer will be provided with a Lighthouse script that requires execution from inside the Azure tenant by an admin to complete the setup process. Claranet will require the Customer's Azure admin to perform this task.
The Customer will be required to grant "Security Admin" access to the Defender for Endpoint portal for the SOC Engineering team and SOC Analysts via GDAP request. A Granular Delegated Admin Privileges (GDAP) request will provide Claranet with access to the Customer's Microsoft Defender portal based on the "least privilege principle". There are additional authorisation requests to support Response Actions, these will need to be approved by the Customer's Systems Administrator.

Note: In the event a Pre-requisite Activity is not completed, the delivery of Service may be delayed, quality of Service may be impacted and/or additional costs may be incurred to deliver the Services. In addition, the Service shall not be subject to the SLAs or Service Credits (if applicable) and shall be provided on a reasonable endeavours basis until the above activities are completed.

8. Service Levels

8.1 Response Matrix

Response times shall be based on the level of severity of any issue that may occur; they are as follows:

Category	P1: Critical	P2: High	P3: Medium	P4: Low	P5: Informational
Definition	Critical severity, issue has a critical impact on the Customer and its environment and may have a severe impact on availability, performance or functionality of live Service. Requires immediate action from the Customer (or action has already been taken by the SOC).	High severity, issue has a high impact on the Customer and its environment but currently no or limited live service degradation. Requires immediate action from the Customer (or action has already been taken by the SOC).	Medium severity, issue may moderately impact the Customer or its environment and requires action from the Customer (or action has already been taken by the SOC).	Low Severity, information ticket. No action required from the Customer, but it should be brought to its attention.	No severity. No action required from the Customer and no need for it to be brought to its attention (non-security issue, BAU, benign, false positive etc.)
Triage	Triaged within 30 minutes of the creation of the first ticket relating to an incident.	Triaged within 30 minutes of the creation of the first ticket relating to an incident.	Triaged within 30 minutes of the creation of the first ticket relating to an incident.	Triaged within 30 minutes of the creation of the first ticket relating to an incident.	Triaged within 30 minutes of the creation of the first ticket relating to an incident.
Response time	Notification within 15 minutes from the point of classification.	Notification within 30 minutes from the point of classification.	Notification within 2 hours from the point of classification.	Notification within 4 hours from the point of classification.	Not applicable.
Notification process	Notification via Claranet Online with a follow up telephone call.	Notification via Claranet Online with a follow up telephone call.	Notification via Claranet Online.	Notification via Claranet Online.	Not applicable.
Ticket Closure	P1 incident tickets will never be set to auto resolve.	P2 incident tickets will never be set to auto resolve.	P3 incident tickets will be set to resolved after 5 days. The tickets will remain open in Claranet Online where they can be responded to by the customer. After a further 3 days with no response, the ticket will close.	P4 incident tickets will be set to resolved after 3 days. The tickets will remain open in Claranet Online where they can be responded to by the customer. After a further 3 days with no response, the ticket will close.	P5 incident tickets closed by the Cyber SOC Team.
Triage SLA Service credit	2.5% of the Monthly Service Fee	2.5% of the Monthly Service Fee	2.5% of the Monthly Service Fee	2.5% of the Monthly Service Fee	2.5% of the Monthly Service Fee
Response SLA Service credit	5% of the Monthly Service Fee	2.5% of the Monthly Service Fee	N/A	N/A	N/A

* In instances where duplicate tickets are created for an incident. The triage time for the first ticket relating to that incident will be used.

In the event that a Customer claims that Claranet did not meet its Service Level Agreement, Claranet will verify such claim and if verified, Claranet shall raise a credit note to the Customer's account and shall be applied to the next invoice in their billing cycle Service Credits will be based on the applicable percentage of the monthly Fee. The maximum amount of Service Credit a Customer can receive in each calendar month relating to this Agreement is limited to 25% of the Monthly Fee for the affected Service. Such Service Credits are pre-agreed liquidated damages and, unless stated otherwise in the Agreement, such Service Credits will constitute the Customer's sole and exclusive remedy with respect to the breach of SLAs.

9. Usage Based Services

This section provides how usage-based Defender agents element of the Service will be billed by Claranet.

Claranet reserves the right to automatically invoice, and the Customer shall pay, for any usage/consumption of Services by the Customer that is either out of the scope of the Service or above any agreed minimum commitment as set out in the applicable Order Form.

The Customer will permit Claranet, or persons designated by Claranet, at Claranet's cost, to audit the Customer's usage and/or consumption at any time, to ensure compliance by the Customer with the scope of the Service or the agreed minimum commitment under any applicable Agreement. Any such audit shall be conducted during regular business hours and in such a manner to not unduly interfere with the normal business activities of either party. If the audit reveals an over usage or underpayment of the Services, the Customer shall, within five (5) business days of a receipt of an invoice, pay any shortfall. If such underpayment is more than 20% for the audited period, the Customer will further pay, or reimburse Claranet for the cost of the audit, as professional services fees.

However, this Service offers a high level of flexibility which allows the Customer to include new endpoints as required. Claranet will manage all endpoints that have met the required pre-requisites, such as the Microsoft license and associated Agent installed as described in this document. The Customer can elect to do either of the following:

(1) **Option 1**: Keep a flexible model by paying only for what is used above the minimum committed endpoints based on the on-demand price of £11.95 per end points/Agents per month ("**On-Demand Price")** or

(2) **Option 2**: The Customer may increase its minimum committed Agents and take advantage of the lower Service Agents pricing available, by Change Request or a new Order Form.

With the Service, the Customer commits to a minimum number of Agents as outlined in the Order Form for an Initial Term. If endpoints are added over and above the minimum committed Agents, then the Customer will be invoiced in arrears following its usage report for the month(s) for such additional Agents in the relevant month(s), based on the applicable On-Demand Price for the Service Agents.

Any increase to the minimum committed Agents will be co-termed with the existing Service remaining Term. For the avoidance of doubt, in the event the Customer elects to increase the Service minimum committed Agents under Option 2, the Service minimum committed Agents cannot be reduced thereafter and the Customer will be liable for such increased commitment until the end of the applicable Initial Term.

As the Service is scalable and provides for a "pay as you go" On-Demand Price option, the Customer is entitled to discounts for committing to a higher number of in-scope endpoints rather than leaving it on the flexible On-Demand Price that is billed in arrears.

10. Delays and Cancellation Terms

1. Professional Services Fees if applicable as part of delivery must be used within six (6) months from the date of Customer's signature of the Order Form and at expiry of this period, Claranet may invoice the full remaining Professional Services Fees and the Customer will pay those Fees in accordance with the Agreement. Thereafter, the Customer will have a further six (6) months to use those remaining Professional Services to deliver the Services, after which they will expire on such date if unused. Unless agreed otherwise, Professional Services are non-refundable.

2. The Customer agrees and acknowledges that Claranet will estimate the time required to complete the Services and that additional days of Professional Services may be required to complete the delivery of the Services. Claranet shall notify the Customer where it determines in good faith additional days are required to complete the Services and such additional days may then be authorised by the Customer in accordance with an additional Order Form.

3. Notwithstanding the above, if delivery is delayed or put on hold by the Customer (expressly or impliedly) after the date of signature for a cumulative period of:

   (a) 1 (one) month, the delivery status will be reviewed for viability;
   (b) 2 (two) months, the delivery status and viability will be reviewed, the project will be marked as "at-risk"; and
   (c) 3 (three) months, Claranet reserves the right to cancel the delivery and invoice the Customer for the greater of (a) any Services delivered up to the point of such cancellation, or (b) the amount payable pursuant to Clause 4.2 of the MSA.

4. If the Customer postpones or cancels a booking (e.g. a workshop, meeting or a call) at short notice, then the following will be charged by Claranet, depending on the amount of notice given:

Notice for Postponement or Cancellation	Postponement or Cancellation Fee
Less than 15 working days but greater than 10 working days	50% of the Fees associated to the booking
Less than 10 working days but greater than 5 working days	75% of the Fees associated to the booking
Less than 5 working days	100% of the Fees associated to the booking

5. If the Customer seeks to cancel a Service/s before the expiry of the Initial Term or Renewal Term, Claranet will automatically invoice and the Customer shall pay for cancellation charges equivalent to the total Fees that would otherwise be payable for the remainder of the Initial Term or Renewal Term of the respective Service/s, unless agreed otherwise.

6. Once the cancellation has been processed by Claranet, the Customer shall follow Claranet's reasonable instructions to decommission any hardware and to cease access to relevant systems that the Customer received as part of the Service.

11. Assumptions and Exceptions

Service delivery may be affected if the following occur below. Where relevant and to the extent any Service Levels set out herein are impacted by the below, Service Credits will not apply as a result.

(1) It is assumed that where required as part of the Service, access to the Customer's IT infrastructure is quickly established and retained for the duration of the Service. Any issues relating to access and permissions may result in work being halted or delayed until such access is resolved, or cause failures in delivery because Claranet personnel are unable to access the Customer's relevant sites.

(2) Where software licences are not provided as part of the Service, it is the Customer's responsibility to ensure it has the appropriate subscriptions and licences as required to benefit from the Service. The costs of such licences and subscriptions are not included in the price of the Service as set out in this Service Description unless otherwise provided in the Agreement.

(3) Claranet is not responsible for any failure of any component for which Claranet has no control over or is not entirely within Claranet's control, including but not limited to electrical power sources, networking equipment, computer hardware, computer software, licences, agents or website content provided or managed by the Customer.

(4) Claranet excludes responsibility for meeting any Service Levels to the extent that meeting the Service Level is affected by the following exceptions hereunder and Service Credits will, therefore, not be paid if the outage occurs from such exceptions:

(a) if the Customer is in default under the Agreement;
(b) in the event that the Service is unavailable due to any component, event or situation not wholly within the control of Claranet, including but not limited to a failure of a component that Claranet is not responsible, electrical power sources, networking equipment, computer hardware, computer software or website content provided or managed by the Customer;
(c) in respect of any non-availability which results during any periods of scheduled maintenance or emergency maintenance;
(d) in the event that the Claranet Service itself is disrupted or unavailable due to viruses, unauthorised users or hackers, not as a result of Claranet's failure, actions or inactions;
(e) in the event that the Service is unavailable due to changes initiated by the Customer, whether implemented by the Customer or by Claranet on its behalf;
(f) in the event that the Service is unavailable as a result of the Customer exceeding system capacity;
(g) in the event that the Service is unavailable due to the Customer's failure to adhere to Claranet's implementation, support processes and procedures;
(h) in the event that the Service is unavailable due to the acts or omissions of the Customer and its employees, agents, contractors or otherwise;
(i) in the event that the Service is unavailable due to Customer's third party contractors or vendors or anyone instructed by the Customer gaining access to Claranet's network, control panel or to the Customer's website at its request;
(j) in the event that the Service is unavailable due to a force majeure event;
(k) in the event that the Service is unavailable due to any violations of Claranet's Acceptable Use Policy;
(l) in the event that the Service is unavailable due to the Customer's negligence or wilful misconduct or of others authorised by the Customer to use the Services provided by Claranet;
(m) in the event that the Service is unavailable due to any failure of any component for which Claranet is not responsible, including but not limited to electrical power sources, networking

equipment, computer hardware, computer software or website content provided or managed by the Customer;

(n) in the event that the Service is unavailable due to any failure of local access facilities provided by the Customer;

(o) in the event that the Service is unavailable due to the Customer's negligence or wilful misconduct of the Customer or others authorised by the Customer, to use the Services provided by Claranet;

(p) in the event that the Service is unavailable due to any failures that cannot be corrected because the Customer are inaccessible or because Claranet personnel are unable to access the Customer's relevant sites;

(q) the Customer's failure to adhere to Claranet's implementation, support processes and procedures;

(r) any failure of local access facilities provided by the Customer;

(s) any periods of scheduled maintenance or emergency maintenance; and

(t) unauthorised users or hackers, or due to any violations of Claranet's Acceptable Use Policy.

12. Terminology

Unless otherwise specified, capitalised terms used in this Service Description shall bear the same meanings as those used in the Master Service Agreement, unless otherwise expressly stated herein. Set out below are a description of key technical terms used in this Service Description.

Terms	Definition
Indicator of Compromise (IOC)	An Indicator of Compromise (IOC) is evidence of potential intrusion on a host system or network.
Tactics, Techniques and Procedures (TTP)	Tactics, Techniques and Procedures (TTP) describe the behaviours of threat actors. Tactics are the high-level description of the behaviour, techniques explain the general method used to achieve the goal, and procedures offer the steps used to carry out the attack.
Event	An action or occurrence that has been recognised and recorded by a log source such as operating system, server, firewall etc. These Events are fed to SOC Analysts who will determine if they are an Incident.
Incident	An Event that has been determined that it may indicate a compromise to the customers security and requires further investigation.
Detection Rules	These are the rules that will be run on the Events that are fed into Claranet Online and the SOC Analysts for further investigation.
Agent	The Agent collects various security-related configuration details and event logs from connected machines, and then copies the data to the Customer's Log Analytics workspace for further analysis. The detection rules are then run on these to determine if further investigation is required by the SOC Analysts. Examples of such data are: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, and logged in user.

Advanced Hunting	Advanced hunting is a Microsoft Defender, query-based threat hunting tool that lets the Customer explore up to 30 days of raw data. Claranet can proactively inspect events in the Customer's network to locate threat indicators and entities.
SOC Analysts	A CREST accredited team of L1 and L2 Security Analysts who operate on a 24/7 basis, providing Incident notification and Incident management. The analysts will investigate the Incidents that have been generated, close false positives, enrich confirmed Incidents and provide remediation recommendations. The Incident details are delivered via Claranet Online.
SOC Engineers	SOC Engineers are available to support the operational components of the in life Service, this includes assisting with onboarding new agents, decommissioning agents or troubleshooting issues with agents.
SOM	The Security Optimisation Manager (SOM) will be assigned to your account and will perform Quarterly Service reviews with you.
Security, Information and Event Management (SIEM)	Platform that enables security personnel to detect threats and respond to security Incidents. For this Service, Claranet uses Microsoft Sentinel, integrated with Microsoft Defender products, to collect and analyse log data so Claranet Security Analysts can investigate Incidents and block malicious activities.
Asset Verification Form	The Asset Verification Form details the log sources that are to be monitored by the Service. This is a living document and will be updated as new log sources are onboarded through the change management process.
Data Tier	This is the amount of Event log data that is fed into the SIEM by the customers log sources.
Managed Service	The XDR service that the SOC team deliver to the customer through incident triage and response and the Engineering team deliver through platform support.