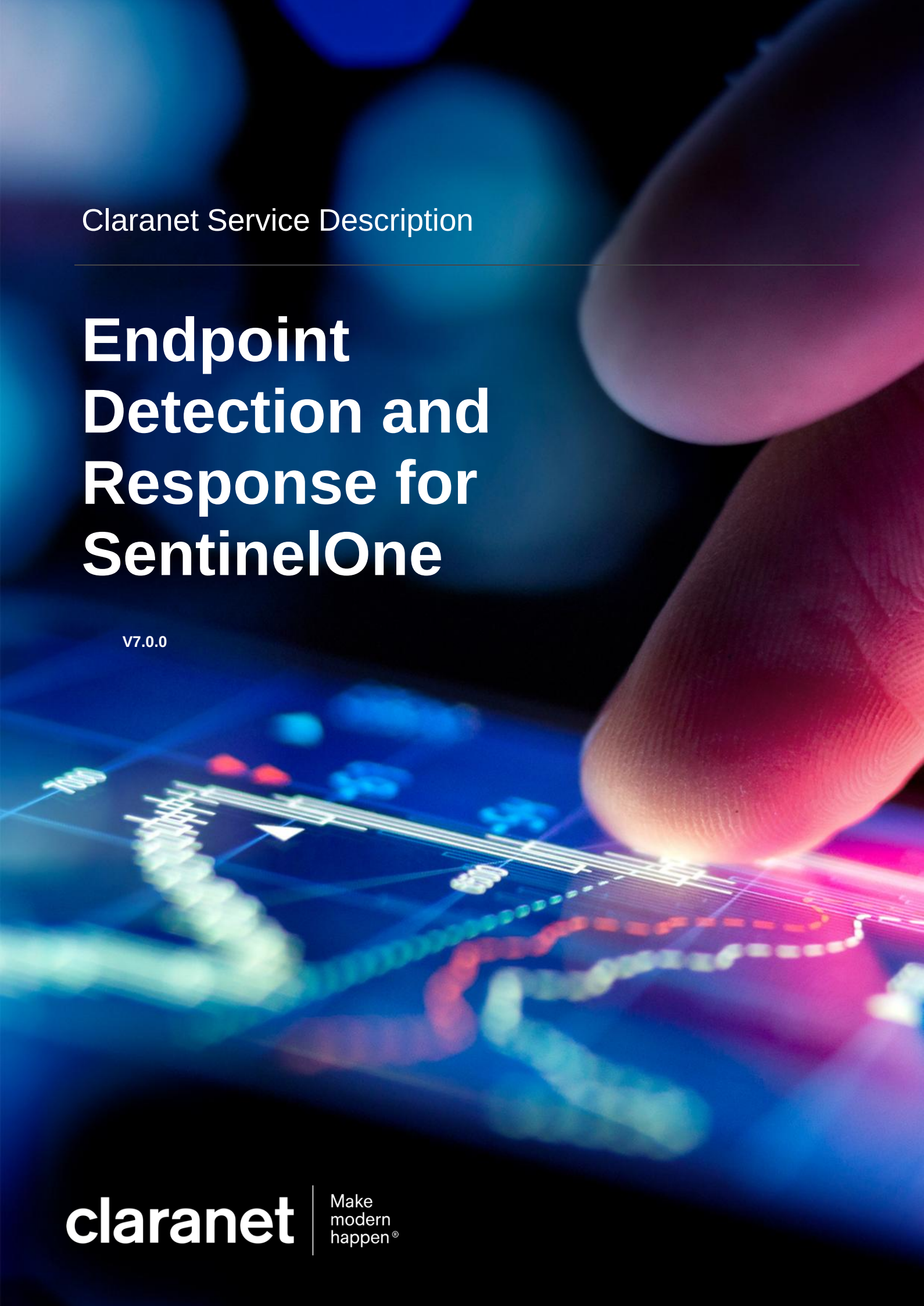

Claranet Service Description

Endpoint Detection and Response for SentinelOne

V7.0.0

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 Endpoint Detection and Response for SentinelOne ("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 Claranet Cyber Security Endpoint Detection and Response for SentinelOne Service ("EDR") provides prevention techniques and response actions to confirmed threats, and in-depth investigation and remediation to suspicious activity, protecting the Customer's network 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.
SentinelOne Singularity Console	SentinelOne Singularity Console is a cybersecurity platform providing endpoint protection, identifying and mitigating threats in real-time. The Customer will have access to change and amend settings such as USB and Bluetooth control. However, the Customer will not have access to change any settings that would impact Claranet's ability to deliver the Managed Service.
SentinelOne Agent	The SentinelOne Agent will be installed on each endpoint to be protected, and it collects device activity data from connected machines, and then copies the data to the SentinelOne Singularity Console for further analysis. The detection rules are then run on these to determine if further investigation is required by the Security Operation Centre (SOC) Analysts.
Assisted Installation	The SOC Engineers will aid system administrators in deploying the agents onto the Customer's endpoints, once the agent is installed and deployed communications will be validated between the agent and Claranet Online. In some cases, firewall changes may also be required to allow communications.
Incident Detection	Telemetry is received from Endpoints on the Customer's infrastructure. If the Events meet the criteria of a detection rule, an Incident ticket will be created which is then reviewed and prioritised by SOC Analysts according to the Response Matrix in the Service Levels section.
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 Incident Notification levels, please see section 8.
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 arranging calls with

	the Customer, and to discuss the attack in more detail with members of the Customer's team if required.
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 perform one hunt per tactic per week, and should anything be found within the Customer's environment, an Incident ticket will be raised. SOC Analysts will develop hypotheses around how a threat actor may have infiltrated the Customer's environment and what the threat actor may be doing once inside. Hunting queries are then developed to manually search for evidence to support the hypotheses. For example, if the analyst has hypothesised that an attacker may have used a remote access tool to gain access, they will look for evidence of remote access tools being used.
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 requires the Customer's feedback using the Incident ticket on whether or not an alert is legitimate to allow Claranet to tune efficiently. SLAs will not be tracked for any alerts being tuned prior to the Service going live.
Detection Rules	The Service will be configured with SentinelOne's standard default policy that can be altered as the Service evolves. The standard default policy applied is to: • Block known threats; and • Raise suspicious detections for analysis. There could be situations where all known and suspicious activities need to be blocked by default. This will be discussed in the scoping meetings. Detection Rules will be defined during the workshop phase of the onboarding process and configured by SOC Engineers to ensure that the Managed

	Service is configured in a way that best protects the Customer's organisation. and endpoints while allowing for business continuity.
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. Disruption will be discussed with the Customer prior to commencement and minimised wherever possible.
Platform Support (Monday to Friday	SOC Engineers are available to support the operational components of the in-life Service from 09:00hrs to 17:30hrs GMT, excluding public and bank holidays. 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 SentinelOne on the Customer's behalf and work with SentinelOne 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 SOC Analysts 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	The Service includes data retention of all security incident information for 365 days and includes 14 days of detailed device activity data for threat hunting or in-depth investigation.

5. Service Operation

This Service shall be read in conjunction with the Cyber Security Service 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. 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 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. Including, a designated Services contact as a decision-maker for a subset of operational issues pertaining to the Claranet Endpoint Detection and Response 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. This includes notifying the SOC of any changes to your account within the management portal such as new users or leavers from the business. Timely notification to allow the SOC to remove or add accounts is required to ensure privilege access is removed or granted. Claranet SOC assumes no responsibility for the misuse of accounts that have not been correctly maintained by the Customer.
Safeguarding Credentials	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.
Security testing	The Customer must notify Claranet of any planned penetration testing or other similar services that may impact this Service, and

	Claranet must approve prior the commencement of any such services. This is because these penetration tests and other similar 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 an uplift of up to 50% of the monthly Fees in the relevant month, which the Customer agrees to be as pre-agreed additional charges for the additional effort.

Third Party Terms and Conditions

As part of the Agreement with Claranet, the Customer's Service will be provided in accordance with the Terms of Service between SentinelOne and the Customer in relation to its use of the SentinelOne software as part of the solution or Service provided by Claranet.

The Customer agrees to and confirms that it has read and understand that it is bound by the SentinelOne's Terms of Service set out herein in relation to the Services/software, which can be found at: https://www.sentinelone.com/terms-of-Service/.

The Customer agrees to and confirms that it has read and understand the SentinelOne Data Privacy Policy and activities set out therein in relation to the SentinelOne software, which can be found at: https://www.sentinelone.com/privacy-policy/.

The Customer acknowledges and agrees that in taking this Service from Claranet that the Customer has been given access to, have read and agree to SentinelOne's Support Terms that apply to its use of the Services/software as part of the Service or solution that Claranet are providing under this Service Description, which can be found here: https://www.sentinelone.com/legal/support-terms/.

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 technical information managed by the Customer that is required for the delivery of the Service by Claranet.
The Customer will provide a mechanism for the roll out of the SentinelOne Agent across its network, such as SCCM, PDQDeploy
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 must provide Claranet with a list of key contacts, including a distribution email address, that will respond to the security incidents via the Claranet Online portal and be responsible for the incidents through to closure.
The Customer must provide information regarding the process and behaviour of its endpoints on the network and disclose the nature of the endpoint and the role it plays within the business. This will aid in the configuration and response actions that the SOC are able to provide on the assets as well as tuning and whitelisting.

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.

7. Service Levels

7.1 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	Threats to critical systems and/or high-value users that may not have been mitigated by either the tool or the SOC, and/or could be part of a wider incident. This may pose an immediate and/or on-going risk. This requires further investigation and/or an immediate and comprehensive response by the Customer.	Threats to critical systems and/or high-value users that may have been mitigated by either the tool or the SOC, and/or are unlikely to be part of a wider incident. This may require further investigation and/or remediation by the Customer.	Threats to non-critical systems and/or users that may have been mitigated by either the tool or the SOC. This may require further investigation and/or remediation by the Customer.	Threats from benign activities or unusual behaviour on non-critical systems or users. This may include misconfigurations and legitimate activity alerts.	This may refer to false positives or routine activities on non-critical systems or users, where it is non-threatening. This may include standard tasks, routine scans, and minor policy deviations. This will require no intervention or verification by the SOC team, but tuning may be required.
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.

8. Usage Based Services

This section provides how usage-based Services will be billed by Claranet. The prices provided below are subject to change, without prejudice to any rights within the MSA, from time to time to reflect costs incurred by Claranet from third parties or suppliers.

The Service offers a high level of flexibility which allows the Customer to organically on-board new devices and install the agent as required. For the avoidance of doubt, each device with an agent installed will constitute an individual licence. 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. If devices are added over and above the minimum committed licences then the Customer will be invoiced in arrears following their usage report for the month(s) for such additional licences in that month(s), based on the applicable On-Demand Price for EDR Service licences. Further, the Customer can elect to do either of the following:

Option 1: Keep a flexible model by paying only for what is used above the minimum committed licences for £11.95 per licence ("On-Demand Price") or

Option 2: The Customer may increase its minimum committed licences and take advantage of the lower Service licence pricing available, by Change Request or a new 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 relating to 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.

When the EDR Service minimum committed licences are increased, this does not impact the Initial Term of the EDR Service, any increase to the minimum committed licences will be co-termed with the existing EDR Service Initial Term. For the avoidance of doubt, in the event the Customer elects to increase the EDR Service minimum committed licences under Option 2, the EDR Service minimum committed licences cannot be reduced thereafter, and the Customer will be liable for such increased commitment until the end of the Initial Term.

Unless the Customer notifies Claranet that it would like to increase its minimum committed licences under Option 2 in accordance with the Change Request process, Claranet will invoice the Customer monthly in arrears for any over usage above the EDR Service minimum committed licences based on the On-Demand Price.

The pricing for On-Demand Price over usage and smaller volume minimum committed licences is significantly greater than larger minimum committed licences for the EDR Service. This is to cover the additional effort of set-up, reporting and onboarding activities. Claranet reserves the right to amend the On-Demand Price.

As the EDR 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 EDR Service licences rather than leaving it on the flexible On-Demand Price that is billed in arrears.

9. Delays and Cancellation Terms

9.1 Professional Services Fees 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.

9.2 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.

9.3 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.

9.4 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

9.5 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.

9.6 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.

10. 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.

10.1. 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.

10.2. 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.

10.3. 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.

10.4. 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:

10.5. if the Customer is in default under the Agreement;

1. 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;
2. in respect of any non-availability which results during any periods of scheduled maintenance or emergency maintenance;
3. 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;
4. 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;
5. in the event that the Service is unavailable as a result of the Customer exceeding system capacity;
6. in the event that the Service is unavailable due to the Customer's failure to adhere to Claranet's implementation, support processes and procedures;
7. in the event that the Service is unavailable due to the acts or omissions of the Customer and its employees, agents, contractors or otherwise;
8. 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;
9. in the event that the Service is unavailable due to a force majeure event;
10. in the event that the Service is unavailable due to any violations of Claranet's Acceptable Use Policy;

11. 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;
12. in the event that the Service is unavailable due to any failure of local access facilities provided by the Customer;
13. 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;
14. the Customer's failure to adhere to Claranet's implementation, support processes and procedures.

11. 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.
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.
CXMS	Customer Experience for Managed Services