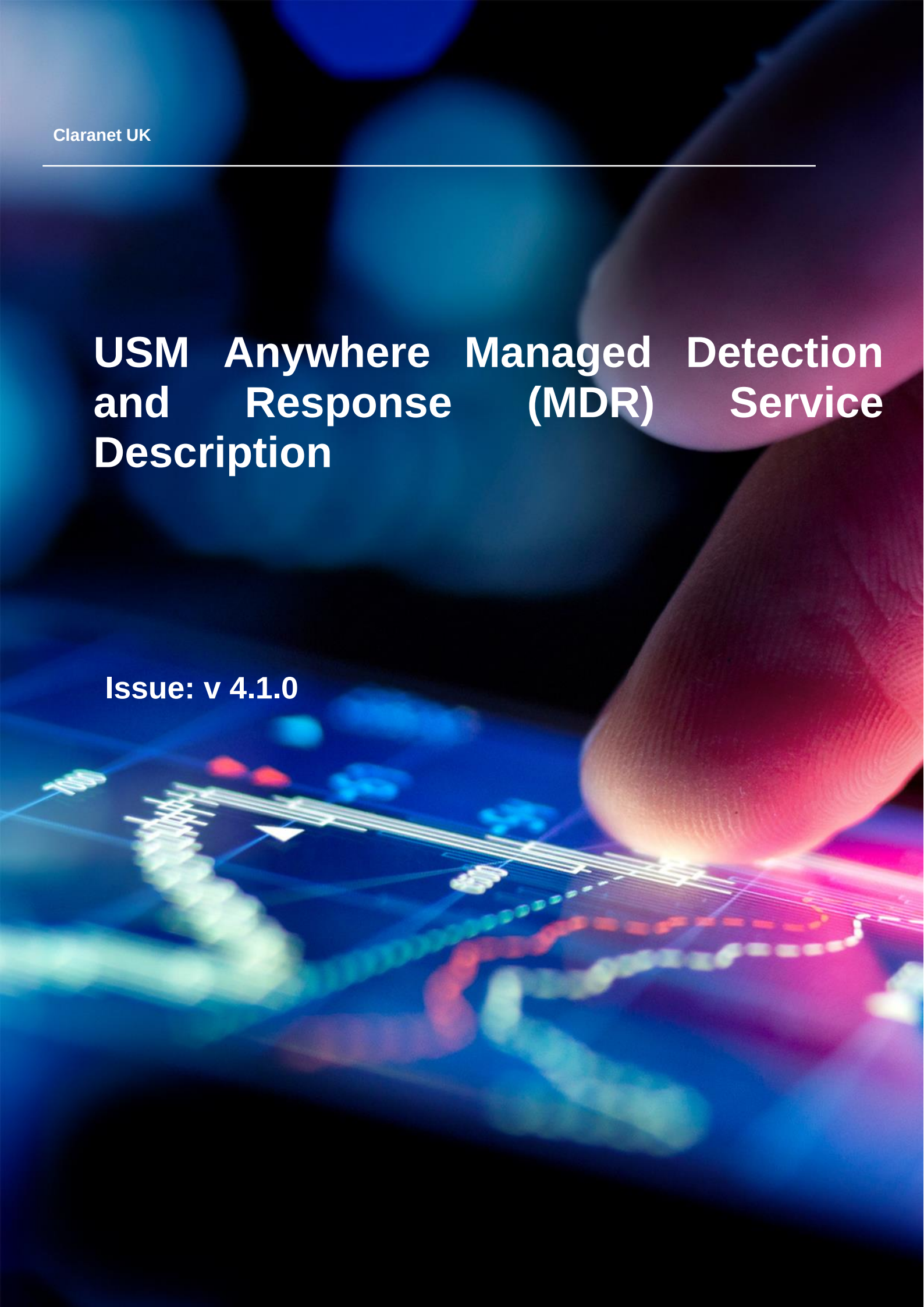
Claranet UK

USM Anywhere Managed Detection and Response (MDR) Service Description

Issue: v 4.1.0



Contents

Version control

Version	Author	Date	Purpose/Change
4.1.0	Shane Aisbett	22.12.2023	General update across the document

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 is subject to the terms of the Claranet Master Services Agreement 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 Master Services Agreement.

Claranet provides the following services as part of its Managed Detection and Response (MDR). The Service components of the Service are set out below along with the related tasks and responsibilities.

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 costs 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 any of the following; Change Request, Order Form, SOW, or at the request or at the direction of the Customer, the 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

Claranet's Managed Detection and Response (MDR) Service provides real-time analysis of security Events that are generated by applications, network devices, hardware, and endpoints on the Customer's network, alerting it to potential risks or breaches. The Customer will receive remediation advice on a 24/7/365 basis from skilled Security Analysts enabling it to contain even the most complex threats to its organisation.

4. Service Features

4.1. Standard Features

The following features are supported as standard:

Feature	Description
Licensed Software	Claranet will retain all configuration rights, and will manage the licensing, of the USM Anywhere Management Console as provided by AT&T.
Claranet Online	The Claranet Online portal is the primary contact point for the Service. Whenever there is a new Incident ticket that requires the Customer's attention or access to the Monthly Reports, the Customer will receive a notification from Claranet Online. This is the location where the Customer will raise queries or respond to Incident tickets if required.
USM Anywhere Management Console	The MDR Service uses a cloud-based, highly-available Security, Information and Event Management (SIEM) platform (USM Anywhere), which is external to the Customer's network. The Customer will be provided read-only access to the USM Anywhere Management Console. This is where all the information the Customer may need to support Incident investigation log data that is being collected, perform searches on the data, run compliance reports, manage asset and vulnerability scans, and create custom dashboards.
Log storage and archiving	Within the USM Anywhere Management Console, log storage and archiving is provided with the solution for the duration of the contract. With the Log storage feature, Claranet will have the ability to search logs that are stored online for a period of 30 days, hereafter, referred to as 'hot log storage'. With the Log archiving feature, Claranet will have access to offline logs, hereafter, referred to as 'cold log storage', which can be used in investigations after uploading the appropriate logs into the system for analysis, which will impact the length of time required to perform an investigation. By default, these logs will be stored in a UK data centre.
Incident Detection	Event information, received from log sources on the Customer's network, are sent to the USM Anywhere Management Console. 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 Incident Response matrix.
Incident Notification	The Customer will receive Incident Notifications for Priority 1 to Priority 4 Incidents in Claranet Online. While the Customer does not receive a notification of Priority 5 Incidents directly, the totals are displayed in the monthly reports on Claranet Online.

	For more detail on the Notification levels, please see the “Service levels and service credits” section.
Incident Management	Claranet will make recommendations on prevention techniques, root cause analysis (as far as the analysts can go with the log investigations), identifying the initial attack vector and provide remediation techniques. This includes attending calls with the Customer and with members of the Customer’s team to discuss the attack in more detail.
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 the Dark Web, other customer deployments, and working closely with other security business units within the Claranet group. This information is fed into the USM Anywhere Management Console and used by the SIEM to enrich Incident investigations. The Analysts will review the Incidents and follow the notification path based on the priorities outlined in “Service priorities and categories” section.
Threat Hunting	Threat hunting involves Claranet’s 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. Claranet Analysts will develop hypotheses around how a threat actor may have gotten into 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. Claranet 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.
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 expected activity, to allow us to tune efficiently.
Standard Detection Rules	All Detection Rules that come with the USM Anywhere Management Console are automatically applied to the Customer Service.
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	Once per calendar quarter, Claranet’s Cyber SOC Team will conduct a Quarterly Service Review with the Customer. During this meeting

	both parties will discuss the Incidents processed, break downs of false positives / benign Events vs Incidents, SLA metrics that have been met, service improvement recommendations, etc.

4.2. Optional Features

The following features are optional, which can be added to the Customer's Service and will be subject to additional charges:

Feature	Description
Asset Scanning	This is a self-managed feature where the Customer can run one-off scans, or schedule it as needed, with the results displayed in the USM Anywhere Management Console. The asset scanner will run a scan to discover hosts deployed on the network. The USM Anywhere Sensor sends Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), and Transmission Control Protocol (TCP) requests to discover hosts on the network to which the sensor is connected.
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 ordered once Acceptance into Service is completed under the Change Management process.
Intrusion Detection	Intrusion Detection comes with built-in Cloud Intrusion Detection (CIDS), Network Intrusion Detection (NIDS), and Host Intrusion Detection (HIDS) systems. This monitors the Customer's traffic and hosts, along with user and administrator activities, looking for anomalous behaviours and known attack patterns, which may result in an Incident. Intrusion Detection will monitor a port mirror for core switches, which can be done at the boundary or an internal core switch. The design considerations will be discussed during the scoping phase and will highlight the benefits of any recommended approach.
Network Vulnerability Scanning	The Network Vulnerability Scanner can perform authenticated and unauthenticated scans on internal network devices (excluding support external scanning of web application or IP addresses). It provides a prioritised dashboard via the USM Anywhere Management Console and will display the severity of the vulnerability, the affected software, and the availability of any patches.
Dark Web Monitoring	Dark Web Monitoring detects if the Customer's end users' credentials have been compromised in a third-party breach and trafficked on the dark web, so that the Customer can take immediate action to prevent a further breach.

	Events are triaged for escalation. This is available for one domain and up to 10 email addresses external to the primary domain.
Hot log storage	While 30-day hot log storage is standard, both 90- and 180-days options are available.

5. Scoping and Solution Design

5.1. Scoping

Claranet will work with the Customer to establish the scope of the Service and provide an indicative quotation and proposal.

5.1.1. Scene Setting call

Claranet will start the process with a scene setting call, during which the Customer's high-level project drivers, goals, and requirements, and how the Service can assist in meeting these will be established.

5.1.2. Scoping Form

The Customer will then be provided with a Scoping Form which gathers information about the type and quantity of the relevant log sources the Customer would like to monitor. It is extremely important to complete the form accurately as errors can lead to underestimating or overestimating the Data Tier leading to insufficient storage (lost logs) or an increase in the cost. Claranet will help the Customer complete this form.

Once the Scoping Form is complete, Claranet will provide the Customer with an indicative quote for the Service.

Responsibility	Claranet	Customer
Scene Setting call: Meeting to gather initial information regarding specific requirements.	✓	
Scoping Form: Provide details of the type and quantity of all log sources to be included in the scope.		✓
Indicative Quotation: Provide pricing including costs for the installation, configuration and tuning of the system; licence costs, and monthly managed service charges.	✓	

5.2. Solution design

If the Customer agrees to proceed, then Claranet will start work on the solution design and finalise the quotation.

5.2.1. Solution Workshop

A Claranet Solution Architect will arrange a workshop with the Customer to understand its technical requirements, the devices that are deemed to be in scope, including count and location, the number of sensors to be deployed, data storage, Data Tier estimate, log sources and the relevant features to be enabled, design considerations as well as any other supporting information required to produce the final design.

5.2.2. Statement of work

Once the contract is confirmed, the Statement of Works (SOW) will be finalised, using all the requirements gathered from the Customer and, where applicable, any third parties, colleagues, or any other relevant source.

The SOW will also contain a clear Success Criteria defined for Service deployment.

5.2.3. Order placed

Once agreement is in place regarding the scope of the service as documented in the SOW, pricing will be finalised, and the order can be placed.

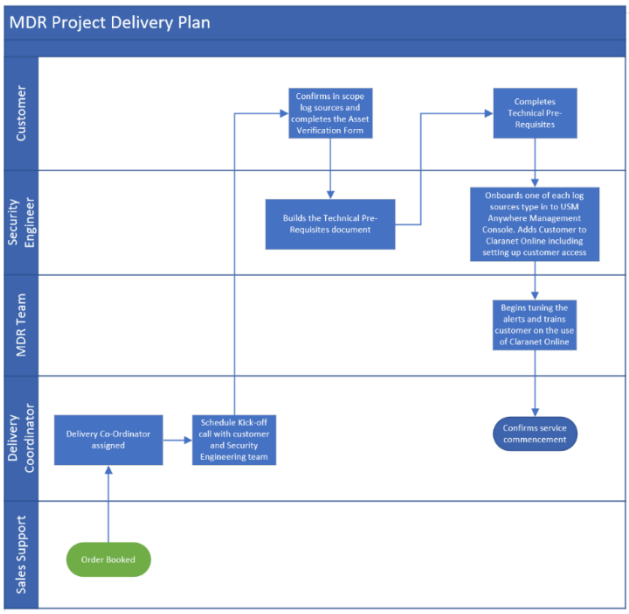
Responsibility	Claranet	Customer
Solution Workshop: Claranet will organise a workshop by conference call to validate and capture technical requirements for the SOW.	✓	
Statement of Works (SOW): The SOW will form part of the contract and will be updated upon any change requests during the contract period.	✓	
Final Quotation: Claranet will provide a final quotation based on the SOW.	✓	

6. Onboarding

6.1. Project Management & Plan

Unless agreed otherwise in the SOW, a Delivery Coordinator will be allocated to coordinate the onboarding of the Service.

6.2. Delivery Plan



6.3. Onboarding

Onboarding of the Service typically takes 12 weeks, but will be dependent upon the size and complexity of the Customer's estate and the completion of the Technical Pre-Requisites within 4 weeks.

6.3.1. Delivery kick off call

Onboarding starts with a kick-off meeting where Claranet's engineers will discuss with the Customer, in detail, the log sources that are in scope to be monitored by the Service. The Customer will then use this information to complete an Asset Verification Form detailing the log sources to be onboarded.

6.3.2. Asset Verification Form

All log sources to be monitored will be documented in the Asset Verification Form, which will be tracked against the SOW to ensure that there will be no discrepancies. If Claranet identifies a change in scope, it will be managed by Change Request.

6.3.3. Technical Pre-requisites

Claranet will use the Asset Verification Form to create a set of Technical Pre-requisite instructions that the Customer can use to configure the Customer's log sources.

The Customer will be required to configure log sources and network topology in accordance with the Technical Requisites instructions. This will allow the logs to be forwarded to the sensors, connectors or USM Anywhere Management Console.

Responsibility	Claranet	Customer
Delivery kick off call: Claranet will set up a kick-off meeting with the Customer.	✓	
Asset Verification Form: The Customer will complete the Asset Verification Form.		✓
Technical Pre-requisite instructions: Claranet will create the Technical Pre-Requisite instructions.	✓	
Technical Pre-requisites: Prior to onboarding any log sources, the Customer must complete the Technical Pre-Requisites.		✓

6.3.4. Onboarding log sources & service features

Once the technical pre-requisites are in place, Claranet engineers will assist the Customer with onboarding one of each type of in scope log sources. As the log sources are onboarded, tuning will begin.

After 30 days, regardless of whether onboarding is complete, including but not limited to the Customer's delay on preparing log sources for onboarding, Claranet may commence billing for the Service (the "Service Commencement Date").

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 SOW and Asset Verification Form.

Responsibility	Claranet	Customer
Tuning: Remove the false positives being generated on the system to establish a baseline of the network and increase accuracy in detection. Tuning will be an ongoing part of the Service, and additional tuning of Events may occur during remediation and notification.	✓	
Tuning sign off: All tuning and filtering actions will be raised within an Incident ticket for approval. Where no		✓

response is received, agreement will be assumed.	
Features and functionality: Claranet will ensure the availability of the solution's features and functionality of the detection element, such as the Network IDS, Asset Detection, Event Correlation and Reporting. The configuration options will be removed from the Customer's view and the Cyber SOC Team will retain all configuration rights and views. Administration accounts will not be provided, unless under special agreement and the business justification identified.	✓

6.3.5. Claranet online

Claranet will provide the Customer with access to the Claranet Online portal, including training on how to use it to interact with the Service. The Claranet Online portal will be configured to allow authorised security personnel to view security related Incidents. Users will also have the ability to update tickets and consult with the Cyber SOC Team as part of this function. Responses are stored on ticket information to provide full auditing of communications and actions taken on an Incident. This can also help to identify weakness in the Customer's Incident response capability.

Access to the Claranet Online portal is for authorised users only, who will be defined in the scoping phase. The Customer should not share user accounts or give these accounts to third parties. Once user accounts are created, the Customer will be able to manage these accounts directly through Claranet Online portal.

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.

7. Scheduled Maintenance

7.1. USM Anywhere Management Console Maintenance

From time to time, maintenance may be performed on the USM Anywhere Management Console, including, but not limited to, hotfixes and Service updates. Within these maintenance windows, the Service may be unavailable for a period of time, during which the log data will be stored and backed up on the sensor. After these maintenance windows, whether or not the maintenance succeeds, the log data will be sent to the USM Anywhere Management Console. If the Customer so chooses, it can receive these maintenance notifications directly for these from AT&T.

7.2. Customer Maintenance

If the Customer has a Service outage (planned or otherwise) with regards to the sensors deployed, they will be responsible to notify the Cyber SOC Team. If no notification is given and the sensors are taken down for

any reason, then the outage will be treated as an Incident. If the sensor is offline for a period, there is a high probability that Events will be lost during the time the sensor is offline.

Responsibility	Claranet	Customer
USM Anywhere Management Console maintenance: Claranet will configure maintenance notification to a distribution group email address that the Customer provides.	✓	
Customer Maintenance: The Customer will be required to notify Claranet if there will be any outage that will impact the sensors deployed on the Customer's network.		✓

8. Change Management

Claranet shall request written approval from the Customer before a change can proceed to be implemented and if any specific time for implementation is required. Below is a list of Change types:

Change type	Definition	Example Changes
Simple Change Request (SC)	A simple change is one that carries a low impact on the Service or business operation.	• Change or removal of key contact(s). • Change or removal of access to the monitoring platform. • Rule suppression, for example, the Customer determines that a P1-4 ticket is standard business practice. • Request for information
Complex Change Request (CC)	A complex change is one that carries a moderate to high impact to the Service or business operation. Where Claranet deems a change to be complex (warranting specialist engineering or excessive time and resources to plan and execute), then Claranet may advise on a charge for these requests.	• Custom rule request. • Additional log sources to be monitored. • Extraction of log history. • Assistance with the removal of elements of the systems from the Customer's environment.

	Claranet will assist in making clear as to whether or not a given request is determined to be chargeable.

8.1. Adding additional log sources

Adding log sources to the Customer's Service may impact its Data Tier and will be subject to additional charges as per Section 10 of this Service Description, for which the Customer shall be liable whether or not; (1) such changes have been accepted by Claranet, and/or (2) such changes were intentional or unintentional.

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. Subject to Claranet's acceptance, these additional log sources will be added to the SOW.

Before Claranet can start monitoring all Customer Events on a newly requested log source, the technical pre-requisite activities must be completed for the additional log sources 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. All additions will be recorded on the Asset Verification Form.

Any additional log sources that do not go through the change process and is not accepted by Claranet will not be monitored and will be considered out of scope.

9. Service

9.1. Cyber SOC Team

9.1.1. Analysts

A CREST accredited team of L1 and L2 Security Analysts who operate on a 24/7 basis, providing Incident notification and Incident management as per the matrix under section 9.5.2.1. 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.

9.1.2. Engineers

The Engineering team are available to support the operational components of the in life Managed Service, this includes onboarding new log sources, decommissioning legacy log sources or troubleshooting issues with active log sources, agents, API/Syslog connections, sensors and the USM Anywhere Management Console. In addition, the Engineering team will also investigate and apply log filtering opportunities on the Customer's behalf.

Where the Engineering team cannot directly resolve an issue, they will escalate any platform issues to AT&T on the Customer's behalf and work with AT&T to resolve the issue.

9.2. Points of contact

Purpose	Who to contact	Contact Info
Support Primary	Cyber SOC Team	https://online.uk.clara.net (Primary)
Support Secondary	Cyber SOC Team	Phone: 0330 390 0500 (Secondary)
Platform Support	Cyber SOC Team	https://online.uk.clara.net (Primary)

9.2.1. Escalations

If the Customer needs to escalate a ticket, Claranet is ready and available to help quickly bring the issue to closure. Within each level of the escalation path, they will be responsible for evaluating the situation, facilitating the resolution plan, and acting as the Customer's sponsor.

An escalation may be initiated when, after working through Claranet standard support processes and with Claranet teams, the Customer is not satisfied with the level or timeliness of the service they have received.

Escalation	Contact	Contact Info
Level 1	Service Desk	+44 (0) 3303 900 500
Level 2	Duty Manager	+44 (0) 3303 900 509
Level 3	Director of Customer Support	+44 (0) 3303 900 505
Level 4	CX & Managed Service director	+44 (0) 3303 900 503

9.3. Hours of Service

Service	Hours of Operation
Security Operations Centre	24/7/365
Engineering	Monday to Friday 09:00 - 1730 GMT excluding UK public holidays

Escalations and complaints	Monday to Friday 09:00 - 1730 GMT excluding UK public holidays

9.4. Service KPIs and metrics

Deliverable	Target delivery time	Delivery method
Monthly Report	Within the first 7 days of the calendar month	Published to the reporting section of Claranet Online portal
Quarterly Review	Within a month following the end of the calendar quarter	Video Call with a member of the Cyber SOC Team

9.5. Service Levels

If Claranet fails to deliver the stated Service level, Claranet agrees that the Customer shall be entitled to receive Service Credits as set forth in this section against the fees owing to Claranet under the Agreement.

9.5.1. Service level availability guarantee

Service levels are set out in the table found under section 9.5.2.2. Please note that a breach of an SLA is not in itself a breach of the Agreement.

9.5.2. Service level credits

In the event that the Customer and Claranet agree that a Service Credit is due in a given calendar month, Claranet will credit the Customer's account with a Service Credit. Service Credits shall apply only to the fee(s) for the affected Service(s). Service Credits shall be deducted from the relevant monthly fee due in the following month when an agreed Service Credit is claimed. The maximum amount of Service Credit a Customer can receive in each calendar month relating to this agreement is fixed to 25% of the Fee for the affected Service. The Service Credits issued are liquidated damages and, unless otherwise provided in the Agreement, such Service Credits will constitute the Customer's sole and exclusive remedy with respect to the breach of SLA's.

9.5.2.1.Service priorities and categories

Category	P1: Critical	P2: High	P3: Medium	P4: Low	P5: Informational
Data exfiltration	Successful access to restricted files and folders, evidence of file modification, deletion, and exfiltration. **Example:** Successful authentication Event, followed by file transfer, destructive behaviour, tampering.	Successful access to restricted files and folders, indicators of file modification but not deletion or exfiltration. **Example:** User account previously failing now has access restricted files and folders and has made change to a file.	Successful access to restricted files and folders following on from failed attempts or sudden change to user settings. No indication of file modification or exfiltration. **Example:** A user account previously failing has now been granted access to a server/files/folders. No evidence of file tampering has been detected. Potential successful escalation of privilege.	Attempted but unsuccessful access to restricted files containing PII data. **Example:** Attempt to access restricted files and folders, failed logon to restricted server. Potential failed attempt to escalate privilege.	No information was exfiltrated, changed, deleted, or otherwise compromised – False positive. **Example:** Authorised user, successful access, non-malicious detection/behaviour.
Unauthorised access	Root/Administrator account compromised and successfully used to log in to a controlled device following previous suspicious activity.	Multiple failed logins for multiple user accounts followed by a successful login attempt by one indicated user. If the successful attempt also performs administrative tasks sudo's to root, escalate to P1	Multiple failed logins for multiple user accounts. This could indicate usernames have been exposed and automated brute force attempts areongoing.	Multiple failed login attempts by the same user, no indication of a successful Event afterwards. No indication of a successful brute force attempt.	Single failed login attempt, normal behaviour, user used the wrong credentials. False positive, non-Event.
Denial of Service	Customer is experiencing total loss of Service during the Denial of Service attack. Web applications are offline. Increase monitoring for other attacks.	High levels of network traffic being received, web applications are intermittently responding, network devices are beginning to become overwhelmed by requests. Clear signs that a Denial of Service is ongoing.	Substantial increase in network activity, web services are responding but at a slower rate than normal. Enough to suggest potential early warning signs of a Denial of Service attack.	Unusual increase in network traffic, not impacting the Service but could indicate other malicious activity.	Increased traffic on the network. Normal activity, non-Service impacting.

Malware	Widespread infection, ransomware, the customer is experiencing Service issues due to the malware being present. Loss of data is expected. Command and Control communication is successful. Firewall allows traffic through.	Widespread infection, non-Service impacting, no indicators of data exfiltration. No indicators to show Command and Control communication. Anti-Virus is unable to detect but the firewall is blocking traffic attempts.	Multiple machines infected with malware, phishing campaign is successful in infecting multiple hosts, Anti-Virus has detected and is dealing with the infection. The firewall is blocking Command and Control traffic, domains, and IP addresses.	Single machine is infected with malware. Anti-Virus has detected and is dealing with the infection. Commercial known malware not ransomware and a lower threat risk.	Adware or Spyware, low risk. Anti-Virus is able to cleanup and respond to the files
Policy violation	User is accessing illegal or inappropriate material. Further investigation and potential law enforcement involvement is required.	Inappropriate material is being accessed that breaks corporate policy.	Torrenting or downloading mass data that could include malicious files. **Example:** Use of offsite storage such as Dropbox.	Use of software against corporate policy. **Example:** Chat software,streaming of content.	Not applicable
Reconnaissance	Enhanced Scan Levels attempting credentials and SQL arguments with successful compromise. Potential loss of data or successful unauthorised access.	Enhanced scan levels attempting credentials and SQL arguments without successful compromise.	Standard web application. Scan attempting to enter credentials, allfailed.	Standard web application. Scan using burpsuite or similar e.g. OWASP Zap	Standard Automated Scan using Nmap on public facing assets.
Phishing	Widespread or targeted senior employee phishing. Successful connection to Command and Control, successful payload delivery and system compromise.	Widespread or targeted phishing campaign with successful Command and Control communication. Anti-Virus detection andquarantine behaviour.	Multiple employees subject to phishing campaign. Command and Control detection with blocked traffic and/or Anti- Virus detection and response.	One user subject to phishing campaign. Command and Control detection with blocked traffic and Anti-Virus detection.	Blocked or unsuccessful phishing emails being sent to the business.

9.5.2.2.Service levels and service credits

Category	P1: Critical	P2: High	P3: Medium	P4: Low	P5: Informational
Definition	Critical severity, issue has a critical impact on the customer and their 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 their 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 their 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 their attention.	No severity. No action required from the customer and no need for it to be brought to their 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 Managed Service Fee	2.5% of the Monthly Managed Service Fee	2.5% of the Monthly Managed Service Fee	2.5% of the Monthly Managed Service Fee	2.5% of the Monthly Managed Service Fee
Response SLA Service credit	5% of the Monthly Managed Service Fee	2.5% of the Monthly Managed 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.

9.5.3. Compensation claims

Compensation claims must be submitted within 30 days from the point the Customer is made aware of the breach. All claims must be submitted to the appointed Account Manager in writing by email. Requests for support received by the Service Desk by means other than telephone or request ticket (for example, by fax) will be excluded when calculating Service levels.

9.5.4. Exceptions

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

- Where the Service has not been accepted by the Customer or has not been delivered by Claranet;
- Where Claranet has not met an SLA due to Customer's failure to minimise the recurrence of problems;
- Where the information provided by the Customer is incomplete, inaccurate, or out of date;
- Where the Service is disrupted or unavailable due to the Customer's failure to adhere to Claranet's reasonable instructions, implementation, support processes and procedures;
- Where the Customer is in default under the Agreement;
- In the event that the Service is unavailable due to the Customer being subject to cyberattacks;In the event that the Service is unavailable due to any failures that cannot be corrected because the Customer is inaccessible or because Claranet personnel are unable to access the Customer's relevant systems;
- Where any non-availability is caused by any periods of schedule maintenance or emergency maintenance initiated by either Parties;
- 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;
- In the event that the Service is unavailable as a result of the Customer exceeding system capacity;In the event that the Service is unavailable due to the acts or omissions of the Customer and its employees, agents, contractors or otherwise;
- Where third party contractors or vendors or anyone gains access to Claranet's network, control panel or to the Customer's website at the Customer's request;
- In the event that the Service is unavailable due to a force majeure event;

- In the event that the Service is unavailable due to any violations of Claranet's Acceptable Use Policy;
- In the event that the Service is unavailable due to any event or situation not wholly within the control of Claranet;
- 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;
- In the event that the Service is unavailable due to any failure of any Service 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;
- In the event that the Service is unavailable due to the acts or omissions of the Customer, its employees, agents, third party contractors or vendors or anyone gaining access to Claranet's network, control panel or to the Customer's website at its request;
- In the event that the Service is unavailable due to any failure of local access facilities provided by the Customer; and
- In the event that the Service is unavailable due to any failures that cannot be corrected because the Customer is inaccessible or because Claranet personnel are unable to access the Customer's relevant sites.

10. Invoicing

Claranet will automatically send invoices via email to the Customer's specified billing contact/s as per the Agreement. If the Customer requires a different format to the standard invoices, including but not limited to the breakdown of an invoice, would be considered bespoke and would incur additional administration fees. Any additional administration fees shall be calculated on a case-to-case basis and will depend on the complexity of the bespoke request.

In instances where the Customer goes over its contracted Data Tier, the Customer shall be liable for all associated fees until resolution. Notwithstanding the foregoing, the engineering team will reach out to the Customer to discuss options for tuning the alerts to bring it back into compliance with its contracted Data Tier. Should that not be possible, the Customer will be given the option to either remove log sources to bring it back into compliance with its contracted Data Tier or sign a Change Request to the Agreement increasing its contracted Data Tier. For the avoidance of doubt, the Customer shall be liable for the Fees for both its contractual Data Tier and any additional Fees associated with overusage, whether or not this was intentional and/or the Parties have resolved such overusage, and such overusage will be captured in the month following when such overusage occurred.

Further to the above, the following link provides additional detail and examples relating to any over usage, including impact to the Service, which the Customer understands and accepts as additional terms that relate to the Services and the Agreement: **USM Anywhere Updated License Overage Behavior | AT&T Cybersecurity (alienvault.com)**

11. Assumptions

If the assumptions listed below are not met, the Service delivery may be affected and any Service Levels set out herein are impacted, Service Credits will not apply as a result:

- The Customer will provide the necessary support and relevant personnel to ensure the success of the project;
- All work will be carried out remotely with no requirement to visit the Customer's site(s) unless agreed otherwise;
- Claranet will have appropriate access to all systems to successfully complete the project;
- Any changes to the scope could result in a revision to the testing timelines and costs;
- This project will not have an impact on any other existing projects;
- The information provided by the Customer is complete, accurate and up-to-date;
- The Customer will provide reasonable and timely cooperation and follow instructions as required by Claranet;
- The Customer will inform Claranet of any scheduled maintenance or emergency maintenance within reasonable notice that will affect the Service's performance;
- The Customer will ensure that technical details are kept up to date by submitting a Change Form or Asset Verification Form to Claranet to confirm or update its relevant details;
- The Customer will correct problems and minimise the recurrence of problems of which the Customer is responsible for that may affect Claranet from meeting the Service levels.

12. Service Decommission

Once it has been determined that the Service will be decommissioned, the Engineering team will send the Customer the updated Asset Verification Form and instructions on how to decommission the devices within the Customer's estate. Any support, including extraction of logs/history or assistance with the removal of

elements of the system from the Customer's environments, will be handled via the Change Management Process.

Responsibility	Claranet	Customer
Ownership: Claranet will retain all configuration rights for; and will oversee the licensing of the end solution. At the end of the contractual period Claranet will send the Customer instructions to remove sensors. Cloud USM Anywhere Management Console access will be revoked and data at this stage will be securely destroyed. If data is required for compliance, this needs to be identified during the scoping period. Additional charges may apply if this is not part of the initial scoping exercise.	✓	
Decommission: The Customer will be responsible for the decommissioning of the devices within its estate as per Claranet's instructions.		✓

13. 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
Managed Detection and Response (MDR)	Managed Detection and Response (MDR) solution providing 24/7 Incident detection, notification, and management.
USM Anywhere Management Console	This refers to the SIEM software from AT&T that underpins the Service.
Security, Information and Event Management (SIEM)	Platform that enables security personnel to detect threats, respond to security Incidents. For this Service Claranet uses USM Anywhere to collect log data so Claranet Security Analysts can investigate Incidents and block malicious activities.
CREST accreditation	The CREST accreditation means our policies, processes and competencies have passed the rigorous accreditation process.

	All members must complete an application process which examines its quality processes and procedures; compliance with standards compliance (e.g., ISO27001, ISO9001); professional indemnity insurance; contract management; informational security processes; complaint handing and conflict of interest policies.
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.
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.
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 in to the SIEM where Detection Rules and the Cyber SOC Team 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 the SIEM will run on the Events that are fed in to it to determine if they require further investigation by the Cyber SOC Team.
Data Tier	This is the amount of Event log data that is fed in to the SIEM by the customers log sources.
Managed Service	The MDR service that the Cyber SOC team deliver to the customer through incident triage and response and the Engineering team deliver through platform support.

14. Addendum

14.1. Technical onboarding information

The information detailed below covers the standard onboarding requirements will be supported by the technical pre-requisites document that will be supplied during the onboarding phase and will cover onboarding requirements that are specific to the Customer's environment.

14.1.1. Deployment on the Customer's network

On-premises sensors are deployed to collect Event log information, provide the network IDS component of the monitoring solution and scanning capabilities if required.

The sensor is responsible for sending logs to the cloud data deployment for correlation and storage.

Responsibility	Claranet	Customer
Active Directory: Configure active directory to allow access to the sensor and provide credentials that will allow Claranet to configure an authenticated connection.		✓
VMware or Hyper-V: Provide a VMware or Hyper-V environment with 5 free network interfaces per sensor.		✓
Deployment on to the network: Experienced Engineers will assist the Customer to deploy the solution to the network.	✓	
Mirror port: Configure a mirror port on the Customer virtual switch or physical network device, allowing traffic to be cloned to a single port for Network Intrusion Detection.		✓

14.1.2. Configuring log sources

Before Claranet can start seeing all Customer Events, there are certain configurations within the Customer's network that must be in place to ensure that the data store is receiving all of the relevant Event logs.

Responsibility	Claranet	Customer
Endpoint Agent: The Customer will ensure the host receiving the endpoint agent meets the pre-requisites.		✓
Endpoint Agent installation: Claranet will provide deployment scripts to the Customer's nominated contact to install the agents on to its network.	✓	
Data sources: Configuration of data sources output to forward the logs to the sensor.		✓
Graylog Extended Log Format: Configure each Graylog Extended Log Format source with the IP address of the Sensor and the port number as the Graylog host.		✓

14.1.3. Deployment in the cloud

The Service supports sensors in AWS, Azure and Google environments and Claranet's Engineering team can provide the Customer with instruction on how to deploy it in those environments.

Responsibility	Claranet	Customer
Access to the cloud: The Customer will provide access (if needed) to its cloud infrastructure.		✓
Deployment in the cloud: Claranet will provide the Customer with the steps to deploy, register, and configure the sensor once access has been made available.	✓	

14.1.4. Infrastructure setup and changes

Responsibility	Claranet	Customer

Sensor deployment: Claranet will provide the Customer with instructions to deploy the sensors to manage the build and communication between the USM Anywhere Management Console and the service management platforms.	✓	
Infrastructure changes: The Customer will make changes to its infrastructure to ensure the solution is working correctly. This may involve making changes to the firewall configuration to allow ports for communication with log sources andupdate servers etc.		✓
Group policy changes: The Customer will make changes as required to its group policy, network settings, logging settings and levels, and ensure that the solution is working as proposed and is collecting the relevant information.		✓
Service accounts: The Customer will create service accounts as required and ensure that Claranet can access resources under the service account. Multiple accounts may be required depending on the user access management system and the ease of auditing.		✓
Ports and IP addresses: The Customer will allocate external IP addresses as required to allow for remote management of the server(s) and software (e.g. hardware deployments) andinternal IP addresses for the software and hardware that is used to collect logs. The Customer must also provide network addresses for the operation of day-to-day activities. The Customer will configure port mirror traffic and assign it to a port that can be cabled into hardware to activate the IDS capabilities.		✓
Emails and escalations: The Customer must define an escalation process if required with points of contacts that can be contacted in an emergency. In addition, the Customer will configure the necessary email addresses		✓

and accounts to be used for notification purposes.	
Internet connection: The Customer will provide a connection out to the internet that is routable from the sensor deployed zones.	✓

14.1.5. Onboarding Responsibilities

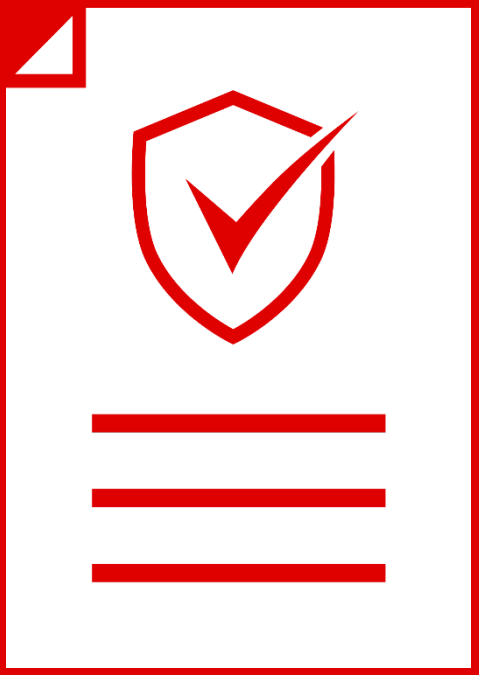
Within the Onboarding process, there are many areas that require configuring to suit the Customer's individual requirements and the specifics of its network. Details of these tasks can be seen below:

Responsibility	Claranet	Customer
Asset scanning preparation: The Customer will provide IP address information and schemas that relate to the operation of the network. The Customer must ensure that the sensor can communicate with the network and that the host based IPS is not blocking the scan. Whitelisting will need to be conducted on all internal protection mechanisms.		✓
Firewall Setup: The Customer will need to configure any firewall or boundary point between its environment and the internet to allow the sensors to transfer data to the cloud data store.		✓
Log source preparation: The Customer will make the relevant changes to the network devices and/or configurations to ensure that the log source onboarding can be met. Any disruption to the onboarding will lead to exceptions being formed to hinder the success criteria of the deployment. The Customer's environment may require updates or upgrades to software packages.		✓

Log source onboarding: Claranet will confirm that the log sources in scope are sending logs to the sensor and the USM Anywhere Management Console. Claranet will also confirm that the log source data is being parsed correctly and the relevant plugins are enabled.. Once one of each type of in scope log sources are onboarded, one part of the success criteria will be met.	✓	
Intrusion detection configuration: The Customer must ensure there are enough free interfaces on both the switch and the ESXI or Hyper-V solution to accommodate the requirements for NIDS deployment. The Customer will configure the switch to mirror traffic from all interfaces and Vlans and will provision the VSwtich or equivalent to ensure the correct interfaces on the sensor are monitoring the traffic. Any failure in this deployment could lead to product features not being enabled.		✓
Intrusion Detection: Claranet will confirm that the port mirror traffic is being monitored and sniffed passively via the sensor, if this is not successful, Claranet will aim to troubleshoot this alongside the Customer. However, if this disruption is caused via a faulty configuration, then the extended deployment time may be chargeable.	✓	
Vulnerability scanning provisions: Provide domain admin level credentials to be used for the authenticated vulnerability scans.		✓
Vulnerability Scanning: Claranet will configure vulnerability scanning groups and test that the vulnerability scanning is working for all hosts, this will require testing of the credentials provided.	✓	
Windows agent requirements: The Customer will ensure that the agent dependencies are met as outlined in the technical pre-requisites. Failure to provide this may result in the product feature		✓

not being made available and/or a reduction in Service or exceptions to the success criteriabeing met.		
Windows agent deployment: Claranet will provide the script for the agent rollout and ensure that agents are associated with the correct end point. For large deployments, Claranet will take a phased approach to agent rollout to ensure accurate association is achieved and ensure the correct monitoring profile is enabled on the agent(s).	✓	
Application agent deployment: The Customer will provide details of all applications, deploy the NXLog community edition application to the relevant endpoint and swap the configuration to the custom provided configuration. The Customer will also ensure that the relevant host can communicate to the sensor via firewall changes both hardware and software firewalls.		✓
Application agent configuration: Applications that are not supported, and need to be identified within the NXLog community edition will require a custom agent to be deployed. Claranet will then confirm Event logs are being received to the USM Management Console system and validate that logs are being normalised.	✓	
Database agent configuration: The Customer will configure the auditing profiles on the databases to be included in the custom parser configuration and ensure endpoints can send data to the sensor via firewall changes either hardware orsoftware or both.		✓
Database agent deployment: Claranet will supply the configuration for the NXLog community edition used to collect the Event database logs. Any application unable to forward syslog by default will require a custom agent	✓	

deployed. Claranet will also confirm Event logs are being received to the system and validate logs are being normalised.	
Threat Intelligence configuration: Claranet will set up threat intelligence to ensure it is configured to run in the Customer's USM Anywhere Management Console.	✓
Integration configuration: Claranet will configure the integration from the USM Anywhere Management Console to Claranet Online ensuring that the data flows through. If the Customer has access to the USM Anywhere Management Console, they will receive a read only account. However, if any configuration changes are made that impact the data integration between the USM Anywhere Management Console and Claranet Online that is a result of changes made, then this downtime or loss of data is not a Claranet responsibility.	✓
Dark Web Monitoring: Claranet will set up one domain and up to 10 email addresses outside the primary domain that enables the Customer to detect if its users' credentials have been compromised in a third-party breach and trafficked on the dark web, so that the Customer can take immediate action to prevent another breach.	✓



Claranet Cyber Security Service Description

Managed Detection and Response for Microsoft Sentinel

v.1.1.1

claranet cyber security

Contents

1

1 Service overview

Claranet provides real-time analysis of security alerts that are generated by applications, network devices, hardware, and end points on your network, alerting you to any risks or breaches.

Cyber-attacks are common. Preventative measures are well understood and are widely adopted in an attempt to block the threat. However, the ability to disrupt an active attack is still out of reach for most organisations. Fast reactions to prevent a potential breach requires a combination of technology and resource. A dearth of expertise and the high cost of sustaining a quality service, means that many organisations are looking to managed security service providers to fill this gap.

The Claranet Managed Detection and Response service for Microsoft Sentinel (or “Microsoft MDR”) provides fast reactions to threats and high-quality alerts enabling you to quickly protect your business and frustrate the attacker’s progress. Analyst driven, we provide real-time investigation of security alerts generated by applications, devices, hardware, and end points on your network. You receive valuable information triaged and analysed by the Claranet Security Operations Centre (or “SOC”), on a 24x7x365 basis, enabling you to contain even the most complex threats to your organisation.

Adaptable to your business goals, the modular service can be delivered to suit everything from compliance drivers to budgetary constraints and augmenting existing capability to advanced threat hunting.

We’ve got you covered.

This Service Description describes the Service Claranet Cyber Security provides and details your (“the Customer”) responsibilities in relation to this Service. This Service Description forms part of an Agreement between the Parties and is subject to the terms of the Claranet Master Services Agreement 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.

The Customer expressly agrees that any services, activities, and deliverables not expressly set out within this Service Description shall be out of scope for the Service. In the event Claranet completes additional services, activities and/or deliverables upon the written request or at the direction of the Customer, the Customer shall be responsible for the payment of all Fees and expenses associated therewith.

1.1 How the service works

Managed Detection and Response comprises four core components:

- Security Incident and Event Monitoring software (SIEM)
- Threat Intelligence feeds
- A team of expert security analysts (Cyber SOC Team)
- User and Entity Behaviour Analytics

There are many levels available (see below) which enables the Service to be tailored to your specific needs and the available levels of technical experience within your company.

1.2 The Managed Detection and Response cycle

There are a number of stages within the Microsoft Managed Detection and Response cycle which ensure that the Service is configured correctly and evolves in line with experience.

Identify: Identify all of the assets within your organisation and to create an understanding of the management of the cybersecurity risk to your systems, data, assets, and your overall capabilities.

Architect: Design the Service to meet your corporate and business goals.

Protect: To monitor all the security events for indicators of compromise.

Response: Build an investigative report that shows what the compromise was and exactly what we found.

Optimise: To continually evolve the system in line with any changes to both internal and external threats.

The quality and depth of your Service is defined by the storage, detection and response options that you choose to build your Service with.

1.3 Storage options

MDR for Microsoft Sentinel is a cloud-based, highly-available SIEM platform, that is external to your network, to house data for 90 days with different options to extend this beyond.

Data storage locations can also be requested based on geographic location, but by default a UK data centre will be selected. The solution uses the same network architecture regardless of customer. Using this framework allows for the ability to scale up or down as required to respond to your business needs.

1.4 Service features summary

Feature	Description
Claranet Online	The Claranet Online portal is your primary contact point for the Service. Whenever there is a new Incident ticket that requires your attention or access to the Monthly Reports, you will receive a notification from Claranet Online. This is the location where you will raise queries or respond to Incident tickets if required.
Incident Detection	Event information, received from log sources on your network, are sent to 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 our Security Analysts according to the Incident Response matrix.
Incident Notification	You will receive Incident Notifications for Priority 1 to Priority 4 Incidents in Claranet Online. While you do not receive a notification of Priority 5 Incidents directly, the totals are displayed in the monthly reports on Claranet Online. For more detail on the Notification levels, please see the " Service levels and service credits" section.
Incident Management	We will make recommendations on prevention techniques, root cause analysis (as far as the analysts can go with the log investigations), identifying the initial attack vector and provide you with remediation techniques. This includes attending calls with you and with members of your team to discuss the attack in more detail.
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 Sentinel Instance and used by the SIEM to enrich Incident investigations. The Analysts will review the Incidents and follow the notification path based on the priorities outlined in "Service priorities and categories" section.

Threat Hunting	Threat hunting involves our 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. Our Analysts will develop hypotheses around how a threat actor may have gotten into your environment and what they may be doing once inside. Hunting queries are then developed to manually search for evidence to support the hypotheses. Analysts will perform one hunt per tactic per week, and should anything be found within your 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. Your feedback via an Incident ticket on whether or not an alert is legitimate expected activity is required to allow us to tune efficiently.
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	Once per calendar quarter, the Cyber SOC Team will conduct a Quarterly Service Review with you. During this meeting we will discuss the Incidents processed, break downs of false positives / benign Events vs Incidents, SLA metrics that have been met, service improvement recommendations, etc.
User Behaviour Analytics	Using native identity connections Claranet will extend protection beyond simple events and actions to cover all users and their behaviour in the organisation. Working with the Customer Claranet will identify key users and systems and monitor for not only events taken by these users but also how the system interacts with them, allowing the Cyber SOC Team to identify outliers and suspicious behaviour before an incident is raised

.

2 Consult

We will work with you to establish the scope of your service and provide an indicative quotation.

2.1 Scene Setting call

We will start the process with a scene setting call, during which we will establish your high-level project drivers, goals, and requirements, and how the Service can assist in meeting these.

2.2 Scoping Form

You will then be provided with a Scoping Form which gathers information about the type and quantity of your log sources you would like to monitor. It is extremely important to complete the form accurately as errors can lead to underestimating or overestimating the Data Tier leading to insufficient storage (lost logs) or an increase in the cost. We will help you complete this form.

Once the Scoping Form is complete, we will provide you with an indicative quote for the Service.

Responsibility	Claranet	Customer
Scene Setting call: Meeting to gather initial information regarding your specific requirements.	✓	
Scoping Form: Provide details of the type and quantity of all log sources to be included in the scope.		✓
Indicative Quotation: Provide pricing including costs for the installation, configuration and tuning of the system; licence costs, and monthly managed service charges.	✓	

3 Design

If you agree to proceed, then we will start work on your solution design and finalise your quotation.

3.1 Solution workshop

Our Solution Architect will arrange a workshop with you to understand your technical requirements, the devices that are deemed to be in scope, including count and location, the number of Sensors to be deployed, data storage, Data Tier estimate, log sources and the relevant features to be enabled, design considerations as well as any other supporting information required to produce the final design.

3.2 Statement of Works

Once the contract is confirmed, the Statement of Works (SOW) will be finalised, using all the requirements gathered from you and, where applicable, any third parties, colleagues, or any other relevant source.

The SOW will also contain a clear Success Criteria defined for Service deployment.

3.3 Order Placed

Once agreement is in place regarding the scope of the service as documented in the SOW, pricing will be finalised, and the order can be placed.

Responsibility	Claranet	Customer
Solution Workshop: We will organise a workshop by conference call to validate and capture technical requirements for the SOW.	✓	
Statement of Works (SOW): The SOW will form part of the contract and will be updated upon any change requests during the contract period.	✓	
Final Quotation: We will provide a final quotation based on the SOW.	✓	

4 Build

Onboarding of the Service typically takes 12 weeks but will be dependent upon the size and complexity of your estate and you completing the Technical Pre-Requisites within 4 weeks.

4.1 Delivery Kick off call

Onboarding starts with a kick-off meeting where our engineers will discuss with you, in detail, the log sources that are in scope to be monitored by the Service. You will then use this information to complete an Asset Verification Form detailing the log sources to be onboarded.

4.2 Asset Verification Form

All log sources to be monitored will be documented in the Asset Verification Form, which will be tracked against the SOW to ensure that there will be no discrepancies. If we identify a change in scope, it will be managed by the Change Request process.

4.3Technical Pre-Requisites

We will use the Asset Verification Form to create a set of Technical Pre-requisite instructions that you can use to configure your log sources.

You will be required to configure your log sources and network topology in accordance with the Technical Pre-Requisites instructions. This will allow the logs to be forwarded to the collectors, connectors, or Sentinel.

Responsibility	Claranet	Customer
Delivery kick off call: We will set up a kick-off meeting with you.	✓	
Asset Verification Form: You will complete the Asset Verification Form.		✓
Technical Pre-requisite instructions: We will create the Technical Pre-Requisite instructions.	✓	
Technical Pre-requisites: Prior to onboarding any log sources, you must complete the Technical Pre-Requisites.		✓

4.4 Onboarding log sources and service features

Once the technical pre-requisites are in place, our engineers will assist you with onboarding one of each type of in scope log source - a process that will normally take 30 days. As the log sources are onboarded, tuning will begin.

After 30 days, regardless of whether onboarding is incomplete due to Customer's delay on preparing log sources for onboarding, the Service and billing will commence.

Thereon, we will continue to work with you to onboard and tune any remaining in scope log sources and features as documented on the SOW and Asset Verification Form.

Responsibility	Claranet	You
Tuning: Remove the false positives being generated on the system to establish a baseline of the network and increase accuracy in detection. Tuning will be an ongoing part of the Service, and additional tuning of Events may occur during remediation and notification.	✓	
Tuning sign off: All tuning and filtering actions will be raised within an Incident ticket for approval. Where no response is received, agreement will be assumed.		✓
Features and functionality: We will ensure the availability of the solution's features and functionality of the detection element, such as, Asset Detection, Event Correlation and Reporting. The configuration options will be removed from your view and the Cyber SOC Team will retain all configuration rights and views. Administration accounts will not be provided, unless under special agreement and the business justification identified.	✓	

4.5 Infrastructure setup and changes responsibilities

Once the technical pre-requisites are in place, our engineers will assist you with onboarding one of each type of in scope log source - a process that will normally take 30 days. As the log sources are onboarded, tuning will begin.

After 30 days, regardless of whether onboarding is incomplete due to Customer's delay on preparing log sources for onboarding, the Service and billing will commence.

Thereon, we will continue to work with you to onboard and tune any remaining in scope log sources and features as documented on the SOW and Asset Verification Form.

Responsibility	Claranet	You

Security Operations Centre: We will deploy the sentinel instance and manage the build and communication between the SIEM and the service management platforms.	✓	
Infrastructure changes: You will be responsible for making changes to your infrastructure to ensure the solution is working correctly. This may involve making changes to the firewall configuration to allow ports for communication with log sources and update servers etc.		✓
Group policy changes: You will be responsible for making changes as required to your group policy, network settings, logging settings and levels, to ensure that the solution is working as proposed and that it is collecting the relevant information.		✓
Service accounts: You will be responsible for creating service accounts as required and ensuring that We can access resources under the service account. Multiple accounts may be required depending on the user access management system and the ease of auditing.		✓
Ports and IP addresses: It will be your responsibility to allocate external IP addresses as required to allow for remote management of the server(s) and software. (Example: Hardware deployments). Allocate internal IP addresses for the software and hardware that is used to collect logs and to provide network addresses for the operation of day-to-day activities.		✓
Emails and escalations: You will have to define an escalation process, if required, with points of contact that can be contacted in an emergency. In addition, you will have to configure the necessary email addresses and accounts to be used for notification purposes.		✓
Internet connection: You will have to provide a connection out to the internet that is routable from the server deployed zones.		✓
Ownership: Upon the expiration of the contract, we will retrieve any hardware assets and may need to access cloud systems to remove Sensors and proprietary rule base. Claranet access to the workspace will be revoked, but any unique configuration and data will remain in the client's Azure tenancy including the Customers Sentinel instance.		

5 Manage

Once configured and in place, the Managed Detection and Response Service will continue to monitor your infrastructure within the agreed scope and notify you of any security events that have been detected. The managed Service comprises many areas that are brought together once the Sensors have been deployed and are passing data to your central data store. These areas have professional analysts to support any automated functionality and provide an enhanced Service.

5.1 Service deliverables

The Managed Detection and Response Service will deliver the following, based on a standard deployment:

- Customer maintenance
- Change management
- Adding additional log sources

Customer Maintenance

If you have a Service outage (planned or otherwise) with regards to the Sensors deployed, your will be responsible to notify the Cyber SOC Team. If no notification is given and the Sensors are taken down for any reason, then the outage will be treated as an Incident. If the Sensor is offline for a period, there is a high probability that Events will be lost during the time the Sensor is offline.

Responsibility	Claranet	You
Customer Maintenance: You will be required to notify us if there will be any outage that will impact the Sensors deployed on your network.		✓

Change Management

We shall request written approval from you before a change can proceed to be implemented and if any specific time for implementation is required. Below is a list of Change types:

Change type	Definition	Example Changes
Simple Change Request (SC)	A simple change is one that carries a low impact on the Service or business operation.	• Change or removal of key contact(s). • Rule suppression for example you determine that a P1-4 ticket is standard business practice. • Request for information

Complex Change Request (CC)	A complex change is one that carries a moderate to high impact to the Service or business operation. Where Claranet deems a change to be complex (warranting specialist engineering or excessive time and resources to plan and execute), then Claranet may advise on a charge for these requests. Claranet will assist in making clear as to whether or not a given request is determined to be chargeable.	• Custom rule request. • Additional log sources to be monitored. • Extraction of log history. • Assistance with the removal of elements of the systems from your environment.
Complex-Contract-Affecting Change Request (CCA)	A complex-contract-affecting (CCA) change is where the request alters the Service in such a way as to no longer operate in the manner set out under the original Statement of Works. CCA's may have an impact on the ongoing billing or commercial agreement of the Service. Claranet will assist in making clear as to whether or not a given request is determined to be complex-contract-affecting. Once a change request is implemented the SOW will be updated and authorised by both parties before being implemented.	• Additional log sources to be monitored that pushes the Data Tier over the contracted limit as stated in the SOW.

Adding additional log sources

Through the change process, you will be able to add log sources to the Service during the contract period by making a request through the Claranet Online portal.

Before we can start monitoring all your 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 you wish to add will be evaluated, configured, and set up correctly.

If you do not notify the Cyber SOC Team, any additional log sources will not be monitored and will be considered out of scope. All additions will be recorded on your Asset Verification Form.

Appendix A

A.1 Optimising your Service

Within the Build process, there are many areas that can be tuned to suit your individual requirements and the specifics of your network. Details of these tasks can be seen below:

Responsibility	Claranet	You
Log source preparation: Make the relevant changes to the network devices and or configurations to ensure that the log source onboard can be met. Any disruption to the onboarding will lead to exceptions being formed to hinder the success criteria of the deployment. The product feature may require updates or upgrades to software packages. When existing Claranet Services are in scope Claranet will assist in completing this task.		✓
Log source onboarding: Confirm that the log sources in scope have been added to the system and are sending logs to the Sensor and Sentinel. Confirm that the log source data is being parsed correctly and the relevant plugins areenabled. Once all assets deemed in scope are onboarded this will meet one part of the success criteria. Claranet will guide the onboarding of the log sources by grouping devices and ensuring a smooth onboarding via a phasedapproach.	✓	

Responsibility	Claranet	You
Windows agent requirements: Ensure that the agent dependencies are met: • 64-bit operating system • PowerShell version 3 at a minimum. Windows OS 10+ • Windows Server 2016+ Admin credentials for the host are provided. Failure to provide this may result in the product feature not being made available and/or a reduction in Service or exceptions to the success criteria being met. When existing Claranet Services are in scope Claranet will assist in completing this task.		✓

Linux agent requirements: Ensure that the agent dependencies are met: • 64-bit operating system • Kernel 5.0+ • Supported Distribution Admin credentials for the host are provided. Failure to provide this may result in the product feature not being made available and/or a reduction in Service or exceptions to the success criteria being met. When existing Claranet Services are in scope Claranet will assist in completing this task.		✓

Responsibility	Claranet	You
Threat Intelligence configuration: Configure the relevant threat intelligence account depending on whether standard or analyst driven option is selected, ensure the data is downloaded and presented in the system ready for use with correlation. A non-exhaustive list of these sources is : OTX, NCSC CiSP, RiskIQ. Claranet review and swap threat feeds throughout the life of the service to ensure a broad range of sources and expertise	✓	

Responsibility	Claranet	You
Integration configuration: Configure the integration from Sentinel to the ServiceNow platform and ensure data is reaching the service management platform. If you have access to the system, you will receive a read only account. However, if any configuration changes are made that impact the data integration between the SIEM and ServiceNow as a result of changes made then this downtime or loss of data is not the responsibility of Claranet.	✓	
Tuning sign off: Sign off of all tuning and filtering actions completed on the system and agree with the baseline that has been set.		✓
Tuning: Tune the system and remove the false positives being generated on the system, this is done to accept a baseline of the network and increase accuracy in detection. Tuning is an ongoing part of the Service and driven by the false positive rate we detect. Any tuning rules will be raised as a ticket and worked with the customer to ensure no rules are put in place that will create blackspots in the detection or otherwise filter out a critical event. .	✓	

A.2 Service priorities and categories

Category	P1: Critical	P2: High	P3: Medium	P4: Low	P5: Informational
Data exfiltration	Successful access to restricted files and folders, evidence of file modification, deletion and/or exfiltration. **Example:** Successful authentication event, followed by file transfer, destructive behaviour, tampering.	Successful access to restricted files and folders, indicators of file modification but not deletion or exfiltration. **Example:** User account previously failing now has access restricted files and folders and has made changes to a file.	Successful access to restricted files and folders following on from failed attempts or sudden change to user settings. No indication of file modification or exfiltration. **Example:** A user account previously failing has now been granted access to a server/files/folders. No evidence of file tampering has been detected. Potential successful escalation of privilege.	Attempted but unsuccessful access to restricted files containing PII or other confidential data. **Example:** Attempt to access restricted files and folders, failed logon to restricted server. Potential failed attempt to escalate privilege.	No information was exfiltrated, changed, deleted, or otherwise compromised – False positive. **Example:** Authorised user, successful access, non-malicious detection/behaviour.
Unauthorised access	Root/Administrator account compromised and successfully used to log in to a controlled device following previous suspicious activity.	Multiple failed logins for multiple user accounts followed by a successful login attempt by one indicated user. If the successful attempt also performs administrative tasks sudo's to root, escalate to P1	Multiple failed logins for multiple user accounts. This could indicate usernames have been exposed and automated brute force attempts are ongoing.	Multiple failed login attempts by the same user, no indication of a successful event afterwards. No indication of a successful brute force attempt.	Single failed login attempt, normal behaviour, user used the wrong credentials. False positive, non-event.
Denial of Service	Customer is experiencing total loss of Service during the Denial of Service attack. Web applications are offline. Increase monitoring for other attacks.	High levels of network traffic being received, web applications are intermittently responding, network devices are beginning to become overwhelmed by requests. Clear signs that a Denial of Service is ongoing.	Substantial increase in network activity, web services are responding but at a slower rate than normal. Enough to suggest potential early warning signs of a Denial of Service attack.	Unusual increase in network traffic, not impacting the Service but could indicate other malicious activity.	Increased traffic on the network. Normal activity, non-Service impacting.

Category	P1: Critical	P2: High	P3: Medium	P4: Low	P5: Informational
Malware	Widespread infection, ransomware, the customer is experiencing Service issues due to the malware being present. Loss of data is expected. Command and Control communication is successful. Firewall allows traffic through.	Widespread infection, non-Service impacting, no indicators of data exfiltration. No indicators to show Command and Control communication. Anti-Virus is unable to detect but the firewall is blocking traffic attempts.	Multiple machines infected with malware, phishing campaign is successful in infecting multiple hosts, Anti-Virus has detected and is dealing with the infection. The firewall is blocking Command and Control traffic, domains, and IP addresses.	Single machine is infected with malware. Anti-Virus has detected and is dealing with the infection. Commercial known malware not ransomware and a lower threat risk.	Adware or Spyware, low risk. Anti-Virus is able to cleanup and respond to the files
Policy violation	User is accessing illegal or inappropriate material. Further investigation and potential law enforcement involvement is required.	Inappropriate material is being accessed that breaks corporate policy.	Torrenting or downloading mass data that could include malicious files. **Example:** Use of offsite storage such as Dropbox.	Use of software against corporate policy. **Example:** Chat software, streaming of content.	Not applicable
Reconnaissance	Enhanced Scan Levels attempting credentials and SQL arguments with successful compromise. Potential loss of data or successful unauthorised access.	Enhanced scan levels attempting credentials and SQL arguments without successful compromise.	Standard web application. Scan attempting to enter credentials, all failed.	Standard web application. Scan using burpsuite or similar e.g. OWASP Zap	Standard Automated Scan using Nmap on public facing assets.
Phishing	Widespread or targeted senior employee phishing. Successful connection to Command and Control, successful payload delivery and system compromise.	Widespread or targeted phishing campaign with successful Command and Control communication. Anti-Virus detection and quarantine behaviour.	Multiple employees subject to phishing campaign. Command and Control detection with blocked traffic and/or Anti-Virus detection and response.	One user subject to phishing campaign. Command and Control detection with blocked traffic and Anti-Virus detection.	Blocked or unsuccessful phishing emails being sent to the business.

Security Incident Process Flow, Service Levels Agreements and Service Credits

Category	P1: Critical	P2: High	P3: Medium	P4: Low	P5: Informational
Definition	Critical severity, issue has a critical impact on the customer and their 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 their 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 their 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 their attention.	No severity. No action required from the customer and no need for it to be brought to their 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 Managed Service Fee	2.5% of the Monthly Managed Service Fee	2.5% of the Monthly Managed Service Fee	2.5% of the Monthly Managed Service Fee	2.5% of the Monthly Managed Service Fee
Response SLA Service credit	5% of the Monthly Managed Service Fee	2.5% of the Monthly Managed Service Fee	N/A	N/A	N/A

Contacting the Security Operations Centre

Purpose	Who to contact	Contact Info
Support Primary	Cyber SOC Team	https://online.uk.clara.net (Primary)
Support Secondary	Cyber SOC Team	Phone: 0330 390 0500 (Secondary)
Platform Support	Cyber SOC Team	https://online.uk.clara.net (Primary)

Operational Hours

Category	Hours
Security Operations Center	24x7 (12 Hour Shift Patten)
Security Engineering	Monday – Friday 09:00 – 17:30
Account Management	Monday – Friday 09:00 – 17:30

Contacting you

Authorised Security Contacts

An authorised security contact is defined as a decision-maker on operational issues pertaining to the Claranet Managed Detection and Response Service. Contact information must be complete in Claranet Online to ensure we contact the correct person.

Designated Services contacts

A designated Services contact is defined as a decision-maker on a subset of operational issues pertaining to the Claranet Managed Detection and Response Service. Claranet will only interface and provide updates to a designated point of contact regarding security incidents dependant on your nomination of the individual or group.

Portal users

The portal users will receive the same access to the portal, setting up individual accounts for the users and notifying them of when an incident is confirmed. Claranet will notify all members of your organisation that have been nominated within the 5-user limit. Should you require more user accounts please contact us to discuss your requirements.

Outages

The Managed Detection and Response Team will be responsible for the Service, if there is any issueimpacting patching or development work scheduled, you will be notified through the portal.

If there is a Service outage (planned or otherwise) with regards to the Sensors deployed, your responsibility is to notify the Managed Detection and Response Team. If no notification is given and the Sensors are taken down

for patching and maintenance of your VMWare or Hyper-V infrastructure, then the outage will be treated as a P1 incident, and a telephone call will be made to whoever the on-call or in hours contact is. If the Sensor is offline fora period of time, there is a high probability that events will be lost during the time the Sensor is offline. Details of outages to the Service will be detailed in the Monthly Service Report.

Common terms used

Terms	Definition
Managed Detection and Response (MDR)	Managed Detection and Response (MDR) solution providing 24/7 Incident detection, notification, and management.
Security, Information and Event Management (SIEM)	Platform that enables security personnel to detect threats, respond to security Incidents. For this Service Claranet uses USM Anywhere to collect log data so Claranet Security Analysts can investigate Incidents and block malicious activities.
CREST accreditation	The CREST accreditation means our policies, processes and competencies have passed the rigorous accreditation process. All members must complete an application process which examines its quality processes and procedures; compliance with standards compliance (e.g., ISO27001, ISO9001); professional indemnity insurance; contract management; informational security processes; complaint handing and conflict of interest policies.
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.
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.
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 in to the SIEM where Detection Rules and the Cyber SOC Team 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 the SIEM will run on the Events that are fed in to it to determine if they require further investigation by the Cyber SOC Team.
Data Tier	This is the amount of Event log data that is fed in to the SIEM by the customers log sources.

Managed Service	The MDR service that the Cyber SOC team deliver to the customer through incident triage and response and the Engineering team deliver through platform support.
Sensor	A log collection utility that may be internal or external to the Customers network.

Service Levels

If Claranet fails to deliver the stated Service level, Claranet agrees that you shall be entitled to receive, in lieu of all other remedies available to you, Service Credits as set forth in this section against the fees owing to Claranet under the Agreement.

Service level availability guarantee

Service levels are set out in the table entitled “Service levels showing priorities and timescales”.

A.2.1 Service level credits

In the event that you and Claranet agree that a Service Credit is due in a given calendar month, Claranet will credit your account with a Service Credit. Service Credits shall apply only to the fee(s) for the affected Service(s). Service Credits shall be deducted from the relevant monthly fee due in respect of the second month following the month in which an agreed Service Credit is claimed. The maximum amount of Service Credit a customer can receive in each calendar month relating to this agreement is fixed to 25% of the fee for the affected Service. The Service Credits issued are liquidated damages and, unless otherwise provided in the Agreement, such Service Credits will constitute your sole and exclusive remedy with respect to the failure for which they are payable.

Compensation claims

Compensation claims must be submitted within 30 days from the point the Customer is made aware of the breach. All claims must be submitted to the appointed Account Manager in writing by email. Requests for support received by the Service Desk by means other than telephone or request ticket (for example, by fax) will be excluded when calculating Service levels..

Exceptions

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

- if you are in default under the Agreement;
- in respect of any non-availability which results during any periods of scheduled maintenance or emergency maintenance;
- in the event that the Service is disrupted due to unauthorised users or hackers;
- in the event that the Service is unavailable due to changes initiated by you whether implemented by you or by Claranet on your behalf;
- in the event that the Service is unavailable as a result of you exceeding system capacity;
- in the event that the Service is unavailable due to viruses;

- in the event that the Service is unavailable due to your failure to adhere to Claranet's implementation, support processes and procedures;
- in the event that the Service is unavailable due to the acts or omissions of you, your employees, agents, third party contractors or vendors or anyone gaining access to Claranet's network, control panel or to your website at your request;
- in the event that the Service is unavailable due to a force majeure event;
- in the event that the Service is unavailable due to any violations of Claranet's Acceptable Use Policy;
- in the event that the Service is unavailable due to any event or situation not wholly within the control of Claranet;
- in the event that the Service is unavailable due to your negligence or wilful misconduct of you, orothers authorised by you to use the Services provided by Claranet;
- 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 you;
- in the event that the Service is unavailable due to any failure of local access to facilities provided by you; and
- in the event that the Service is unavailable due to any failures that cannot be corrected because you are inaccessible or because Claranet personnel are unable to access your relevant sites. It is your responsibility to ensure that technical contact details are kept up to date by submitting a request ticket to confirm or update the existing technical contact details.

A.3 Cancellation of the Service

Responsibility	Claranet	You
Notice of cancellation: Give 90 days' cancellation notice for the Service to Claranet prior to the end of the contract term in writing to the MSP Cancellations team. Any support you need including extraction of logs/history or assistance with the removal of elements of the system from your environments will be charged as time and materials at the current Claranet consulting rate at the time of carrying out the works.		✓