SERVICE DESCRIPTION

Threat Detection

Name	NTT Ltd. Service Description – Threat Detection
Owner	NTT Ltd.
Status	APPROVED
Classification	UNCLASSIFIED-EXTERNAL
Version	V1.3
Date	29 March 2019

Contents

1 Service Matrix

The NTT Ltd. Device Management Enhanced service consists of a core set of Service Modules and associated Service Elements.

Section	Service Modules and Elements		
3.0	Core Service Elements		
3.1	24/7 Hours of Operation	✓	✓
3.2	Security Operation Centers	✓	✓
3.3	NTT Ltd. Portal	✓	✓
3.4	Portal Language Support	✓	✓
4.0	Service Transition		
4.1.1	Engagement	✓	✓
4.1.2	Planning	✓	✓
4.1.3	Staging	✓	✓
4.1.4	Integration	✓	✓
4.1.5	Go-Live	✓	✓
5.1-6.1	Detection Types		
	Advanced Analytics with proprietary machine learning / behavioral modeling	✓	✓
5.1-6.2	Threat Intelligence		
	Services enhanced by NTT Ltd. Global Threat Intelligence Center	✓	✓
	Continuous threat intelligence updates driven by production investigations	✓	✓
5.1-6.3	Security Analyst Interaction		
	Automated analysis	✓	
	Detailed Security Incident investigation by Security Analyst		✓
	Event-driven threat hunting		✓
	Vendor integration and evidence collection for key security technologies[1]		✓
5.4-6.4	Client Notification		
	Automated Security Incident Reports	✓	
	Analyst-created Security Incident Reports based on detailed investigation and threat hunting		✓
5.5-6.5	NTT Ltd. Portal and Reporting		
	Portal	✓	✓
	Client access to Events (90 days)	✓	✓
	Client access to Incidents (lifetime of contract)	✓	✓
5.6-6.6	Service Options		
	[Option] Investigator – Enriched and aggregated log search		✓
	[Option] Secure long-term log storage and management	✓	✓
	[Option] On-premises Point of Delivery (POD)		✓
	[Option] Proactive Response		✓
	[Option] Vulnerability Correlation		✓

[1] *Gathers and analyzes evidence data in relation to vendor alerts, such as PCAPs and execution reports.*

2 Service Prerequisites

2.1 General Requirements

2.1.1 Service Selection

Client is responsible for selecting services and ensuring that the selected services meet the compliance standards (e.g. PCI, HIPAA) applicable to Client operations.

2.1.2 Client Point of Contact

Client will assign a main Point of Contact (POC) to work with the NTT Ltd. Account Team to schedule all service-related activities and communicate with the SOC as needed for installation and ongoing tuning and support.

- To prevent delays during Implementation, Client will ensure completion of the NTT Ltd. Client Security Service Detail (CSSD) form.
- Client (POC) will be available during all scheduled activities.
- Client is responsible for providing NTT Ltd. with all contact information updates pertaining to Incident and Security Incident escalation instructions.
- Client is responsible for maintaining NTT Ltd. Portal user list and rights.

2.1.3 Access and Connectivity Requirements

Client will ensure access and connectivity to all 'in-scope' devices, including the ability to receive source feeds and evidence data (packet capture, stack trace, etc.).

2.1.4 Client Staff and Resources Requirements

Client will provide knowledgeable technical staff, and/or third-party resources, to assist with hardware and software implementations, including:

- Configuring end-to-end connectivity to ensure the successful transport of all in-scope Log feeds and evidence data.
- Providing rack space and power for each in-scope NTT Ltd. Appliance (if applicable).
- Providing an IP address for each NTT Ltd. Appliance to be installed at Client site.
- Installing NTT Ltd. Appliances on Client's network.
- Installing Log Transport Agents (LTAs) – NTT Ltd. will provide the Client with access to documentation via the NTT Ltd. Portal and support in configuration and installation of LTA's during Service Transition
- Participate on Clients calls with third-party vendors and offer support as appropriate.

2.1.5 Source and LTA Configurations

Source device and LTA configurations must comply with NTT Ltd.'s standard setup requirements. NTT Ltd. provides Configuration Guides that provide configuration guidance for supported in-scope devices. If Client's configuration cannot or does not comply with NTT Ltd.'s configuration guidance, engineering consulting hourly rates will apply to develop a custom solution. Additionally, if any devices are not compliant with NTT Ltd. Configuration Guides, including use of supported versions of source devices only, Client agrees in good faith to worktime, NTT Ltd. reserves the right to suspend services for applicable configuration items until the situation is remedied. In such cases no claim for service credit shall be applicable. NTT Ltd. is not responsible for any Incident involving an in-scope configuration item while such privileges are disabled or otherwise non-functional.

2.1.6 Technologies that may impede delivery

If Client utilizes security technologies that block traffic, rotate Logs, or otherwise impede NTT Ltd.'s ability to receive Logs from in-scope devices, Client must notify NTT Ltd., and cooperate with NTT Ltd. to identify a mutually agreed upon mitigation to be developed.

Note: Loss of Log lines and interruption of monitoring capabilities may occur because of uncoordinated Log rotation.

2.1.7 Third-Party Vendors

Client will work directly with its third-party vendors hosting any in-scope devices to allow NTT Ltd. to deliver services.

2.1.8 Maintenance, Support, and Licensing Agreements

Client is responsible for procuring all maintenance, support, and licensing agreements with third-party vendors for all non-NTT Ltd. provided in-scope devices for the term of the Client agreement, unless otherwise stated in the Purchase Order.

2.1.9 Software Modification

NTT Ltd. will not support altered, damaged, or modified software, or software that is not an NTT Ltd.-supported version.

2.1.10 Third-Party Device Failure

Client will work with third-party vendors to rectify device failure for all non-NTT Ltd. provided devices and is responsible for all associated expenses.

2.1.11 Responsibility for Data Privacy, Regulatory, and Administrative Policies and Procedures

Client is responsible for complying with all relevant data privacy, regulatory, and administrative laws and policies and procedures related to monitoring user traffic and communications.

2.1.12 Physical Security of NTT Ltd. Appliances

Client is responsible for ensuring the physical security of all NTT Ltd. Appliances located on-site at Client locations or hosted at third-party locations.

2.1.13 Internet Service Provider or Client Network Outages

Client is responsible for resolving Client Internet Service Provider (ISP) outages, or issues with Client internal network infrastructure.

2.1.14 System Backups

NTT Ltd. recommends that Client performs full backups of relevant systems prior to the performance of services.

2.1.15 Closure of Incidents and Security Incidents

Client will work with NTT Ltd. to bring closure to each Incident and Security Incident identified by the services presented in this Service Description.

2.1.16 Providing Required Information

Client’s failure to provide any of the Service Requirement information on a timely basis can result in delays in Service Transition and Service Delivery by NTT Ltd. and NTT Ltd. shall not be liable for any consequences of such delays.

2.2 Communication Requirements

2.2.1 NTT Ltd. Appliance

Managed Security Services require an NTT Ltd. Appliance. The NTT Ltd. Appliance is available in multiple form factors, including a virtual image and physical appliance. All NTT Ltd. Appliances must be installed, initially configured and enrolled by the Client. NTT Ltd. will only be responsible for management and maintenance of the appliance software (in both physical and virtual form factors) and the physical appliance form factor if supplied by NTT Ltd..

NTT Ltd. Appliances gather Logs, events, reports, and evidence data from in-scope Client devices and systems, then prepare the data for secure transmission and processing. The NTT Ltd. Appliance also provides a secure communication path for Device Management service delivery. Ongoing configuration and maintenance of the NTT Ltd. appliance is conducted by NTT Ltd. and therefore the appliance must be installed by the Client in a suitable location on the Client network infrastructure to facilitate both NTT Ltd. access and log collection.

The NTT Ltd. Appliance requires:

- A static (non-dynamic) RFC 1918 IP address
- Permanent LAN Connectivity
- Permanent Internet connectivity on TCP port 443

For the virtual form factor the NTT Ltd. Appliance also requires:

- Must to be configured to power on automatically if the hypervisor is restarted
- Minimum resources from the hypervisor in the virtual environment as specified by NTT Ltd.

2.2.2 Configuration Item Requirements

All in-scope configuration items require:

- For internet-facing configuration items a static (non-dynamic) public IP address
- For non-internet-facing configuration items – a static (non-dynamic) RFC 1918 IP address
- Necessary network connectivity to NTT Ltd. Appliance as specified by NTT Ltd.

2.2.3 Connection to Client Network

The Client must supply all the necessary network hardware and cabling to connect the configuration item to the Client’s own, third-party and ISP networks. All network interfaces connecting to the configuration items must be a minimum of 1 Gigabit Ethernet interfaces. The standard for Gigabit stipulates auto mode as mandatory. However, some vendors have deviated from this and do facilitate the hard coding of interface speed and duplex. Where this is enabled, it is imperative that both ends of the network cable are set to fixed speeds and duplex modes (in other words both Switch and Configuration Item). In this instance it is important that the Client discusses any potential infrastructure changes that may affect this setting.

3 Core Service Elements

3.1 Hours of Operation

Managed Security Services are delivered through the Security Operations Centers (SOCs) of NTT Ltd.. Unless otherwise stated, MSS hours of operation are 24 hours a day, 7 days a week.

3.2 Security Operation Centers (SOCs)

NTT Ltd. will deliver services from its SOCs. NTT Ltd. may at its sole discretion deliver services from any of its SOCs, and Client data may be held in any of the SOC and MSS platform locations unless there is prior agreement and approval between NTT Ltd. and the Client.

3.3 NTT Ltd. Portal

The NTT Ltd. Portal is a globally available web-based application, which allows Clients to interact with, manage, and monitor Managed Security Services.

3.4 Language support

Services are provided in English language only, unless there is prior agreement and approval between NTT Ltd. and the Client.

4 Service Transition

Service Transition is executed in five phases, these are:

- 1. Engagement
- 2. Planning
- 3. Staging
- 4. Integration
- 5. Go-Live

The five phases and activities and procedures within them, ensure a consistent approach to management and completion of the transition and a framework for governance and communication. During the first four phases of the Service Transition period there will be no alerts, incidents, or cases generated for customer review and triage.

4.1.1 Engagement Phase

To initiate the Service Transition, a Purchase Order is submitted along with the Pricing Information from the approved quotation, a High-Level Design document, and the Client Security Services Detail to NTT Ltd..

- Purchase Order (PO) and
- Pricing Information
- Client Security Service Detail (CSSD)
- High Level Solution Design

NTT Ltd. reviews the provided documentation and confirms that all the requirements for commencement of the transition have been met.

A Kick-off meeting is held to communicate the Transition Process, the project tasks, roles and responsibilities and introduce the key stakeholders.

The Engagement Phase is expected to take 12 business days and can be accelerated if completed and accurate documentation is provided when submitting the Transition Service Request.

4.1.1.1 Engagement Phase Activities

The key activities during the Engagement Phase are as follows:

- Receive the Service Transition Request and PO and respond within three business days
- Review provided documentation within six business days
- Provide feedback and confirm content is complete and aligned to the Service Order
- Assign a Service Transition team including allocation of an NTT Ltd. Security Client Service Manager
- Create the Draft Service Transition Project Plan, including timeline and constraints within 10 business days
- Arrange a Kick-off meeting within 12 business days (if documentation is complete and confirmed)

4.1.1.2 Engagement Phase Deliverables

The deliverables provided during the Engagement Phase are as follows:

- Purchase Order Approval
- Kick-off meeting (face to face or call)
- Draft Service Transition Project Plan, including timeline, standard risks and issues

4.1.2 Planning Phase

The Service Transition Planning Phase validates the provided documentation and locks down the transition plan, scope, and timeline. The Planning Phase is expected to take six business days

4.1.2.1 Planning Phase Activities

The key activities during the Planning Phase are as follows:

- Agree on final architecture, including devices and logs collection
- Assess Log Source Scope and Prioritization, including completing Log Source Inventory where applicable
- Client Approval of Final Service Transition Plan
- Confirm Services Delivery Model, including Incident Management and Steady State Governance

4.1.2.2 Planning Phase Deliverables

The Final Service Transition Plan (including timeline, risks, and issues) is provided as a deliverable during the Planning Phase.

4.1.3 Staging Phase

The Service Transition Staging Phase establishes the primary service elements for NTT Ltd. to provide the service. It includes connectivity, appliances for log collection and device management access, and NTT Ltd. Portal and IT Service Management (ITSM) setup. The Staging Phase is expected to take 12 working days.

4.1.3.1 Staging Activities

- The key activities during the Staging Phase are as follows:
- Install NTT Ltd. Appliances (shipping, if required)
- NTT Ltd. Appliance initial configuration and hardening
- Setup and validation of remote access
- Log(s) events/ monitoring setup (Client device)
- OOB configuration (if applicable)
- SOC Portal account(s) configuration
- SOC infrastructure preparation
- Testing of bi-directional ticket flow , as appropriate.

4.1.3.2 Staging Deliverables

The deliverables provided during the Staging Phase are as follows:

- NTT Ltd. Appliance required to support MSS
- Client credentials for Portal
- Client Entitlement in NTT Ltd. ITSM
- Test results

4.1.4 Integration Phase

The Service Transition Integration Phase completes the required technical service elements for NTT Ltd. to provide the service. It includes configuration of Threat Detection, advanced features for log collection, and final NTT Ltd. Portal and ITSM integration. Additionally, during the Integration Phase, the NTT Ltd. CSM conducts the Welcome meeting and Portal training with the Client. The Integration Phase is expected to take 21 business days.

Following the Welcome meeting, the CSM becomes the interface into the NTT Ltd. services.

4.1.4.1 Integration Activities

The key activities during the Integration Phase are as follows:

- Final validation of connectivity to the SOC
- Device(s), log(s), and service testing and final verification
- Normalization and tuning (logs, not devices)
- Quality assurance review and activation of the service(s)
- Risk and Issue documentation
- Welcome meeting or call with Partners and Client (NTT Ltd. decision)
- Portal training meeting or call with Partners and Client (NTT Ltd. decision)
- Confirm Service Activation Date (in phases, if required), Billing Date, and SLA start date

4.1.4.2 Integration Deliverables

The deliverables provided during the Integration Phase are as follows:

- Client Welcome meeting and Portal training
- Service Activation Date
- Client review and acceptance of the Risk and Issue Register

4.1.5 Go-Live Phase

The Service Transition Go-Live confirms that the service is live and closes the Service Transition Project. The Go-Live Phase is expected to take six working days.

4.1.5.1 Go Live Activities

The key activities during the Go-Live Phase are as follows:

- Operational Check List review by SOC
- Conduct Service Transition Plan closure review meeting or call with Partners and Client (NTT Ltd.S decision)
- Review all remaining open action items including lessons and risks/issues to be considered for Steady State (going forward)
- Receive Partners and Client Service Transition Plan closeout final approval

4.1.5.2 Go-Live Deliverables

The deliverables provided during the Go-Live Phase are as follows:

- Risks/Issues Register (if any)
- Commencement of service and Billing
- Lessons learnt (if any)

4.1.6 Service Transition Deliverable Acceptance

The Service Transition is considered complete on the Service Activation Date and after any Go-Live deliverables are provided. The deliverables are considered as being accepted at the completion of next phase. The Client will close the Service Transition by agreeing to the closure of the parent ticket in ITSM

5 Threat Detection – Standard Features

NTT Ltd. offers two Threat Detection services, Threat Detection – Standard, and Threat Detection – Enhanced.

Threat Detection – Standard (TD-S) is an automated service with no SOC Security Analyst investigation, where threats identified with a certain Confidence are sent directly to Clients in the form of a detailed Security Incident Report that describes the Security Incident with general recommendations that enable Client's Incident Response team to act on the identified activity, reducing the mean time to respond to mitigate the associated risk.

The following sections describes the features of NTT Ltd. TD-S service.

5.1 Detection Type

The TD-S service utilizes Advanced Analytics with proprietary machine learning / behavioral modeling to detect threats in the Client environment. Advanced Analytics leverages a combination of traditional threat detection techniques (e.g. correlation, pattern matching, reputation feeds) with Advanced Analytics (e.g. machine learning, statistical modeling, kill-chain modelling) and Threat Intelligence which enable detection of sophisticated threats.

5.1.1 Severity and Confidence settings

TD-S uses Machine-Learning in identification and reporting of Security Incidents. As NTT Ltd. gains knowledge of emerging/ or evasive threats, the Confidence in accurately identifying these increases over time. Once Confidence has reached levels deemed suitable for automated service delivery, TD-S will start notifying Clients for matching activity.

While using default Severity and Confidence settings is suitable for most Clients, NTT Ltd. allows Clients with specific needs to adjust the minimum Confidence level for which suspicious activity will be deemed a Security Incident and the Client notified.

The minimum Confidence levels are set on a Per-Severity basis (Low, Medium and High), example:

Severity	Min. Confidence (>=)
High	Medium
Medium	Max
Low	Disabled

Altering the Confidence level setting increases, decreases, or disables the service's ability to detect emerging, and evasive threats for the benefit/trade-off of increasing, or decreasing the number of False-Positives, on a per Severity basis.

Severity and Confidence settings are configured during:

- Service Transition described in section '4 Service Transition', by capturing desired configuration in the CSSD.
- Continuous service delivery using Self-Service functionality on the NTT Ltd. Portal.
- Continuous service delivery by submission of a request on the NTT Ltd. Portal.

5.2 Threat Intelligence

The TD-S service is enhanced by Threat Intelligence delivered by the NTT Ltd. Global Threat Intelligence Center.

Additionally, the TD-S service includes continuous threat intelligence updates driven by investigations of actual Security Incidents.

5.3 Security Analyst Interaction

The TD-S service is an automated service, Security Analysts are not involved in normal service delivery.

5.4 Client Notification

TD-S is an automated service. Clients are sent automated Security Incident Report notifications via e-mail.

5.5 Portal and Reporting

TD-S Clients will have access to the NTT Ltd. Portal that includes access to 90 days of Events, and Incidents for the lifetime of Client contract.

5.6 Service Options

5.6.1 Investigator – Enriched and Aggregated Log Search

Client log search is not an option for the TD-S service.

5.6.2 Secure Long-Term Log Storage and Management

TD-S Clients have the option to purchase secure long-term log storage and management.

5.6.3 On-premises POD

TD-S Clients do not have the option for On-premises POD.

5.6.4 Proactive Response

TD-S Clients do not have the option for Proactive Response.

6 Threat Detection – Enhanced Features

NTT Ltd. offers two Threat Detection services, Threat Detection – Standard, and Threat Detection – Enhanced.

In the Threat Detection – Enhanced (TD-E) service suspicious activities and all relevant contextual information are presented to a skilled Security Analyst, who engages in threat hunting and threat validation activities to verify the threat, its impact and to identify additional information associated with the potential breach. Once verified, the Security Analyst creates a detailed Security Incident Report and initiates Security Incident notifications in accordance with documented Client procedures, providing a detailed description of the Security Incident combined with scenario- specific actionable response recommendations, which significantly assist businesses in reducing the time to take informed responsive measures, lowering associated risks.

The following sections discuss the features of NTT Ltd. TD-E service.

6.1 Detection Type

The TD-E service utilizes Advanced Analytics with proprietary machine learning / behavioral modeling to detect threats in the Client environment. Advanced Analytics leverages a combination of traditional threat detection techniques (e.g. correlation, pattern matching, reputation feeds) with Advanced Analytics (e.g. machine learning, statistical modeling, kill-chain modelling) and Threat Intelligence which enable detection of sophisticated threats. To ensure service quality, NTT Ltd. will continuously make detection tuning decisions based on the validity and relevance of service generated Events and Security Incidents.

6.2 Threat Intelligence

The TD-E service is enhanced by Threat Intelligence delivered by the Global Threat Intelligence Center. Additionally, the TD-E service includes continuous threat intelligence updates driven by investigations of actual Security Incidents.

6.3 Security Analyst Interaction

The TD-E service includes detailed Security Incident investigation by Security Analysts in an NTT Ltd. SOC, including threat validation and threat hunting activities across the Client's in-scope log monitoring / telemetry environment to enable validation and assessment of the malicious nature of a threat and its potential impact.

The TD-E service also includes vendor integration and evidence collection for selected security technologies, including packet capture data (PCAP) and malware execution reports. For details on availability refer to technology solutions guides.

6.4 Client Notification

Security Incident Reports for the TD-E service are based on detailed investigation and threat hunting and are prepared by a Security Analyst. Clients are notified based on Client's selection of NTT Ltd. supported notification options, including e-mail and phone calls.

6.5 Portal and Reporting

TD-E Clients will have access to the NTT Ltd. Portal that includes access to 90 days of Events, and Incidents for the lifetime of Client contract.

6.6 Service Options

6.6.1 Investigator – Enriched and Aggregated Log Search

TD-E Clients have the option to purchase NTT Ltd. Investigator log search capabilities. Investigator provides the Client access to an interface to perform historical log searches.

Service option is not available for Clients delivered on On-premises POD infrastructure as described in section '6.6.3 On-premises POD'.

6.6.2 Secure Long-Term Log Storage and Management

TD-E Clients have the option to purchase secure long-term log storage and management.

Service option is not available for Clients delivered on-premises POD infrastructure as described in section '6.6.3 On-premise POD'.

6.6.3 On-premise POD

TD-E Clients have the option to purchase an On-premises POD for scenarios where logs are required, or preferred to remain on-site.

6.6.4 Vulnerability Correlation

TD-E Clients subscribed to NTT Ltd. Vulnerability Management service may benefit from added Vulnerability Correlation capabilities on an opt-in basis.

Feature opt-in request are made during Client Service Transition, or raised by the Client on the NTT Ltd. Portal during continuous service delivery.

Upon opt-in, the NTT Ltd. Vulnerability Management service provides TD-E with added contextual information of Client assets and Vulnerabilities which are then used by Vulnerability Correlation to increase TD-E's overall ability to understand the relevance of a threat and raise the accuracy of Security Incident reports.

6.6.4.1 Service option prerequisites

- TD-E Client is also subscribed to Vulnerability Management services delivered by NTT Ltd. using Qualys.
- Client Qualys subscription includes access to the Qualys API and the API key is provided to NTT Ltd. for integration purposes.
- Client Qualys API subscription is appropriately sized and reflect the size of the organization and its asset estate, smaller subscriptions may result in limited usages caused by Qualys API restrictions.

6.6.5 Proactive Response

TD-E Clients have the option to purchase Proactive Response capabilities. With the Proactive Response add-on option NTT Ltd. shall take actions to contain/disrupt threats described in security incidents, when the Security Analyst deem it appropriate. Actions are performed on Client network devices, typically hindering, or limiting the progress of identified attacks sufficiently to provide the Client with additional time to take informed Incident Response actions.

6.6.5.1 Threat containment

In response to Security Incidents identified by the TD-E service, NTT Ltd. shall take appropriate actions to block threats from traversing Client network devices. Blocking actions are implemented using Indicators of Compromises (IOCs) seen in association of threats.

6.6.5.2 Client acceptance

- Client accepts that Proactive Response actions are of Emergency Change nature and are considered outside traditional change management processes in priority of disrupting/containing threats.
- Client understands and accepts the risks associated with responsive actions and the potential negative impact it may have on the availability of the Client environment.
- NTT Ltd. shall not be held liable for any negative impacts responsive actions within the scope of Proactive Response service options may have.

6.6.5.3 Service option prerequisites

- Client Network Devices are configured in accordance with the NTT Ltd. Configuration Guide.
- Network design and Client's security policy shall be configured in a manner which supports the containment actions provided by NTT Ltd..
- Client Network Devices are provided with access to the NTT Ltd. Incident Response Platform using internet connectivity.

7 Terminologies and Definitions

Terminologies and Definitions for Threat Detection services are presented in the 'NTT Ltd. - Terminology and Shared Services Reference' document that accompanies this Service Description.

8 Operating Level Agreements

Operating Level Agreements for Threat Detection services are presented in the 'Operating Level Agreements – Managed Security Services' document that accompanies this Service Description.

9 Changes in Service

9.1 Regulatory Change Requirements

- If regulatory changes (e.g., changes by a regulatory agency, legislative body, or court of competent jurisdiction) require NTT Ltd. to modify the Services described herein, NTT Ltd. will modify the Services and this Service Description accordingly without diminishing the features, functionality or performance. In the event a modification in response to regulatory changes results in a diminishment of features, functionality or performance, Client agrees in good faith to work with NTT Ltd. to amend this Service Description accordingly and execute any additional agreement which may be reasonable requested by NTT Ltd. to document such amendment.

9.2 Method of Service Delivery

NTT Ltd. reserves the right to make changes to the service, provided these changes do not have a material adverse impact on functionality or performance.

9.3 Modification of Source Feeds

Materially modified source feeds may constitute a coding change to the classifier in use. These changes may result in the re-instigation of the Service Transition process.

Clients subscribed to On-premises POD service option as described in section '7.6.3 On-premises POD' shall ensure that Source feed versioning reflect that of NTT Ltd. Supported Device List and the configuration of these are in accordance with the On-premise POD specific Source Feed Configuration Guides.

9.4 Operating System or Application Alteration

If any of the Operating Systems or applications resident on any of the originally contracted devices are materially altered, NTT Ltd. may re-instigate the Service Transition process, and Classifiers or LTAs may require modification or development.

Clients subscribed to On-premises POD service option as described in section '7.6.3 On-premises POD' shall ensure that Source feed versioning reflect that of NTT Ltd. Supported Device List and the configuration of these are in accordance with the On-premises POD specific Source Feed Configuration Guides.

9.5 Unanticipated Log Volume

Client agrees in good faith to work with NTT Ltd. to amend the contract accordingly, if the Client’s environment generates an inordinate number of Logs or Events processed by the MSS.

10 Service Exclusions

Unless otherwise agreed between the Client and NTT Ltd., the services described in this document do not include the following:

- Configuration of in-scope security systems and devices to allow for Log, Events, and evidence collection.
- Support and Remedial Work which is not expressly stated in this Service Description This includes any troubleshooting and problem solving related to issues arising from Client actions or Client’s network.
- Project Orientated Requests (PORs) are not included in the Services described herein and are subject to additional fees. NTT Ltd. and the Client will develop a scope for the POR and NTT Ltd. will provide a separate quote to Client, which must be executed prior to performance of any such work.
- Client requests for advice or consultation regarding network or configuration item configuration not specifically outlined in this Service Description is not included are subject to additional fees.
- Client staff training unrelated to NTT Ltd. services (NTT Ltd. provides written and video training on the NTT Ltd. Portal and the different functions that Client may use within the portal.).
- Software or hardware maintenance (unless otherwise stated).
- Software licensing (unless otherwise stated).
- Software or hardware upgrades.
- Network connectivity troubleshooting.
- On-site forensic services.
- Security policy or procedure establishment.
- Firewall rule set design, validation and troubleshooting.
- Remediation of a Security Incident or attack on a Client’s network, server or application.

11 Controlling Terms

In the event of any conflict between the terms of this Service Description and the terms of the Client agreements, then terms of this Service Description shall control.

NTT

Together we do great things