Enterprise Security Monitoring

Name	NTT Service Description – Enterprise Security Monitoring
Owner	NTT
Status	APPROVED
Classification	UNCLASSIFIED-EXTERNAL
Version	V1.3
Date	29 March 2019

Contents

1 Service Matrix

NTT Ltd. Managed Services are available in packages consisting of a core set of Service Modules, associated Service Elements and Options.

Enterprise Security Monitoring (ESM) is an NTT Ltd. Managed Security Service (MSS) that utilizes the MSS infrastructure to identify and report on the following categories of Security Incidents:

- **Compliance** – Security Incidents that indicate a deviation from a pre-defined baseline of a regulatory body's definition of compliance controls.
- **Security Best Practices** – Security Incidents that indicate a deviation from a pre-defined baseline of NTT Ltd.'s definition of security best practices.
- **Business Policy Compliance** – Security Incidents that indicate a deviation from a pre-defined baseline of an organization's custom business policy compliance requirements.

NTT offers two levels of Enterprise Security Monitoring services: Enterprise Security Monitoring – Standard and Enterprise Security Monitoring – Enhanced.

- **Enterprise Security Monitoring – Standard** services are designed for organizations with standardized compliance and security best practice monitoring requirements across a core set of security technologies.
- **Enterprise Security Monitoring – Enhanced** services are designed for organizations with customized compliance, security best practice, and business policy enforcement monitoring requirements across a broad set of security technologies.

Section	Service Elements	Monitoring Services	
		Enterprise Security Monitoring - Standard	Enterprise Security Monitoring - Enhanced
3.0	Core Service Elements		
3.1	24/7 Hours of Operation	✔	✔
3.2	Security Operations Centers	✔	✔
3.3	NTT Portal	✔	✔
3.4	Client 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	✔	✔

Section	Service Elements	Monitoring Services	
		Enterprise Security Monitoring - Standard	Enterprise Security Monitoring - Enhanced
5.1-6.1	Detection Types		
	Security Best Practices and basic compliance profile	✔	✔
	Enhanced compliance profile (PCI, HIPAA)		✔
	Customized Event detection		✔
5.1-6.2	Security Analyst Interaction		
	Automated Event analysis	✔	✔
	Custom Event analysis with Security Analyst Verification		✔
	24/7 Security Analyst assistance		✔
5.3-6.3	Client Notification		
	Automated email notifications	✔	✔
	24/7 Security Analyst telephone notifications		✔
5.4-6.4	NTT Portal and Reporting		
	Web portal	✔	✔
	Configurable reporting	✔	✔
	Client access to 90 days of Event and Security Incident data	✔	✔
5.5-6.5	Service Options		
	[Option] Investigator – Enriched and aggregated log search		✔
	[Option] Secure long-term log storage (SLTLS)	✔	✔

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 Client 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 forward/send source feeds to the NTTSA for service enablement.

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.
- Providing rack space and power for each in-scope NTT Appliance (if applicable).
- Providing an IP address for each NTT Appliance to be installed at Client site.
- Installing NTT Appliances on Client network.
- Installing Log Transport Agents (LTAs) – The Account Team will provide Client with documentation and/or support to assist with the installation of all LTAs.
- Working with third-party vendors for support or provide authorization for Account Team to contact third-party vendors on behalf of Client 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 work with NTT Ltd. to amend the Purchase Order accordingly.

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 all valid 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 can 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 perform 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-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 Appliances

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 Appliances

Client is responsible for ensuring the physical security of all NTT 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 perform full back-ups of relevant systems prior to the deployment 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 NTT Ltd. shall not be liable for any consequences of such delays.

2.2 Communication Requirements

2.2.1 NTT Appliance

Managed Security Services require an NTT Appliance.

The NTT Appliance is available in multiple form factors, including a virtual image and physical appliance. All 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 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 Appliance also provides a secure communication path for Device Management service delivery. NTT Appliance ongoing configuration 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 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 Appliance also requires:

- Automatic power-on to be configured in case 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 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 should 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 deliver services at its sole discretion 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 Portal

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

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

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 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
- 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)

4.1.2 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

4.2 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.

4.2.1 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

4.2.2 Planning Phase Deliverables

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

4.3 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 Portal and IT Service Management (ITSM) setup. The Staging Phase is expected to take 12 working days.

4.3.1 Staging Activities

The key activities during the Staging Phase are as follows:

- Install NTT Appliances (shipping, if required)
- NTT Appliance initial configuration and hardening
- Setup and validation of remote access
- Log(s) events/ monitoring setup (Client device)
- OOB configuration (if applicable)
- MSS SOC Portal account(s) configuration
- MSS SOC infrastructure preparation
- Testing of bi-directional ticket flow, if appropriate

4.3.2 Staging Deliverables

The deliverables provided during the Staging Phase are as follows:

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

4.4 Integration Phase

The Service Transition Integration Phase completes the required technical service elements for NTT Ltd. to provide the service. It includes configuration of all purchased services, advanced features for log collection (if applicable) and device management, and final Portal and ITSM integration. Additionally, during the Integration Phase, NTT Ltd. will conduct the Welcome meeting and Portal training with the Client. The Integration Phase is expected to take 21 business days.

4.4.1 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
- MSS SOC Welcome meeting or call with Client (NTT Ltd. decision)
- MSS SOC Portal training meeting or call with Client (NTT Ltd. decision)
- Confirm Service Activation Date (in phases, if required), Billing Date, and SLA start date

4.4.2 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

4.5 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.

4.5.1 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 Client (NTT Ltd. decision)
- Review all remaining open action items including lessons and risks/issues to be considered for Steady State (going forward)
- Receive Client Service Transition Plan closeout final approval

4.5.2 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)

4.6 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 Enterprise Security Monitoring – Standard Features

NTT Ltd. offers two Enterprise Security Monitoring services:

- **Enterprise Security Monitoring – Standard** (ESM-S) services are designed for organizations with standardized compliance requirements across a core set of security technologies.
- **Enterprise Security Monitoring – Enhanced** (ESM-E) services are designed for organizations with custom compliance requirements across a broad set of security technologies.

This section presents the features of the NTT Ltd. ESM-S service.

5.1 Detection Type

The ESM-S service uses a standardized rule and anomaly-based compliance profile to identify and report on the following categories of Security Incidents:

- **Compliance** - Events that indicate a deviation from a pre-defined baseline of a regulatory body's definition of compliance controls.
- **Security Best Practices** - Events that indicate a deviation from a pre-defined baseline of NTT Ltd.'s definition of security best practices.

The NTT Ltd. Standard Rule sets for existing supported device types are included in the ESM-S service. No customized rules creation is included in the ESM-S service. 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.

5.2 Security Analyst Interaction

The ESM-S service utilizes automated detection for high confidence Security Incidents, with Security Analyst verification for other Security Incidents.

5.3 Client Notification

Automated notifications are utilized for the ESM-S service. Clients are notified via NTT Ltd. e-mail systems and can view updates on the portal.

5.4 Portal and Reporting

ESM-S Clients will have access to a web portal that includes access to 90 days of Events and Security Incidents. ESM-S Clients will also have access to monitoring and configurable reporting.

Use of standard NTT Ltd. reports is included as part of the ESM-S service. Development of custom reports is not included as part of the ESM-S service.

5.5 Service Options

5.5.1 Investigator – Enriched and Aggregated Log Search

ESM-S Clients do not have the option to purchase Investigator.

5.5.2 Secure Long-Term Log Storage (SLTLS)

ESM-S Clients have the option to purchase secure long-term log storage.

6 Enterprise Security Monitoring – Enhanced Features

NTT Ltd. offers two Enterprise Security Monitoring services:

- Enterprise Security Monitoring – Standard (ESM-S) services are designed for organizations with standardized compliance requirements across a core set of security technologies.
- Enterprise Security Monitoring – Enhanced (ESM-E) services are designed for organizations with custom compliance requirements across a broad set of security technologies.

This section presents the features of the NTT Ltd. ESM-E service.

6.1 Detection Type

The ESM-E service uses customized rules and an anomaly-based security detection and compliance profiles to identify and report on the following categories of Security Incidents:

- **Compliance** - Events that indicate a deviation from a pre-defined baseline of a regulatory body's definition of compliance controls.
- **Security Best Practices** - Events that indicate a deviation from a pre-defined baseline of NTT Ltd.'s definition of security best practices.
- **Business Policy Compliance** - Events that indicate a deviation from a pre-defined baseline of an organization's custom business policy compliance requirements.

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.

- Use of the NTT Ltd. Standard Rule sets for existing supported device types is included in the ESM-E service.
- Support for devices not currently supported by ESM services may be requested via the Non-Standard Request process (NSTAR) for ESM-E service Clients.
- Up to fifteen (15) Standard or Compound Rules can be developed and implemented annually for ESM-E service Clients.
- Additional Standard or Compound Rules can be purchased via the Move Add Change Delete (MACD) process at a rate of 6 MACD's per rule.
- Up to five (5) existing Analysers can be implemented annually for ESM-E service Clients.
- Additional existing Analysers can be purchased via the Move Add Change Delete (MACD) process at a rate of 12 MACD's per Analyser.
- Development of new Analysers can be purchased via the MACD process at a rate to be determined based upon the level of effort associated with the development of the Analyser.

6.2 Security Analyst Interaction

The ESM-E services utilizes automated detection for high confidence Security Incidents, with Security Analyst verification for custom high priority business use cases.

6.3 Client Notification

A mixture of automated and manually created notifications are utilized for the ESM-E service. Clients are notified based on Client's selection of NTT Ltd. supported notification options, including e-mail and phone calls. Additionally, updates may be viewed on the portal.

6.4 Portal and Reporting

ESM-E Clients will have access to a portal that includes access to 90 days of Events and Security Incidents. ESM-E Clients will also have access to monitoring and configurable reporting.

Use of standard NTT Ltd. reports is included as part of the ESM-E service. Development of custom reports is not included as part of the ESM-E service.

6.5 Service Options

6.5.1 Investigator Client Log Search

ESM-E Clients have the option to purchase NTT Ltd. Investigator log search capabilities. Investigator provides the Client access to an interface to perform investigative searches on enriched logs.

6.5.2 Secure Long-Term Log Storage (SLTLS)

ESM-E Clients have the option to purchase secure long-term log storage.

7 Terminologies and Definitions

Terminologies and Definitions for Managed Security 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 Managed Security 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.

9.4 OS 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.

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 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.

Together we do great things