NTT

Client Service Description

Vulnerability Management Service

01 October 2019 | Document Version 1.6

NTT contact details

We welcome any enquiries regarding this document, its content, structure, or scope. Please contact:

Bob Gordon -Services Product Portfolio Director - Security, Mobile Phone: +1 203 446 4942

NTT Limited
✉ bob.gordon@global.ntt

Please quote reference {Document Reference Number} in any correspondence or order.

Confidentiality

This document contains confidential and proprietary information of NTT Limited ('NTT'). {ClientFull} ('{Client}') may not disclose the confidential information contained herein to any third party without the written consent of NTT, save that {Client} may disclose the contents of this document to those of its agents, principals, representatives, consultants or employees who need to know its contents for the purpose of {Client}'s evaluation of the document. {Client} agrees to inform such persons of the confidential nature of this document and to obtain their agreement to preserve its confidentiality to the same extent as {Client}. As a condition of receiving this document, {Client} agrees to treat the confidential information contained herein with at least the same level of care as it takes with respect to its own confidential information, but in no event with less than reasonable care. This confidentiality statement shall be binding on the parties for a period of five (5) years from the issue date stated on the front cover unless superseded by confidentiality provisions detailed in a subsequent agreement.

Terms and conditions

NTT and {Client} acknowledge and agree is subject to NTT's standard terms and conditions which are available on request. NTT reserves the right to vary the terms of this document in response to changes to the specifications or information made available by {Client}. Submission of this document by NTT in no way conveys any right, title, interest, or license in any intellectual property rights (including but not limited to patents, copyrights, trade secrets or trademarks) contained herein. All rights are reserved.

NTT does not assume liability for any errors or omissions in the content of this document or any referenced or associated third party document, including, but not limited to, typographical errors, inaccuracies, or out-dated information. This document and all information within it are provided on an 'as is' basis without any warranties of any kind, express or implied. Any communication required or permitted in terms of this document shall be valid and effective only if submitted in writing.

All contracts with NTT will be governed by {Law} Law and be subject to the exclusive jurisdiction of the {Law} courts.

top® EMPLOYER GLOBAL 2019
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

Client Service Description

{Subject}

Document Preparation

	Name	Title	Date
Prepared:	Paul Asdagi	Service Director – Group Security	12 Sep 2018
Prepared	Mike Oberholtzer	Sr. Product Manager	01 Feb 2019
Reviewed:	David Bakkers	Business Process Analyst	28 Nov 2018

Release

Version	Date Released	Pages	Remarks
1.0	12 Sep 2018		Internal DRAFT
1.5	01 Oct 2019		Rebrand
1.6	20 Nov 2020		SLA Added

This document is only a general description of the available Services. The Services to be supplied are subject to change. For each Client, the Services will be as set out in the contract entered into by the Client and NTT. If there is any conflict between this docuament and the contract, the contract will prevail.

Table of Contents

List of Figures

List of Tables

1. Service Description

Numerous regulatory and compliance frameworks require organizations to perform vulnerability scanning of key assets, remediate identified vulnerabilities, and develop status reports. Managers and auditors must ensure that their organization’s security posture meets organizational risk management and compliance requirements.

NTT’s Vulnerability Management Service provides the flexibility needed to create a vulnerability scanning program specifically designed to fit an organization’s requirements. Clients choose from a variety of features and options, including internal and external scanning, Payment Card Industry (PCI) scanning, managed or self-service scanning. Other services include vulnerability management architecture review (Placement & Connectivity) and program and plan creation which are supported by Professional Security Services resources.

1.1. Overview

Features of the NTT Vulnerability Management service include the following:

- **External and Internal Scanning Options –** External vulnerability scanning specifically examines an organization's security profile from an external. Internal vulnerability scanning operates your organization’s firewall(s) to identify real and potential vulnerabilities inside your network.
- **Managed or Self-Service Scanning –** Vulnerability Management offers flexibility in scan management – scans can be managed and executed by expert analysts in Security operation centers or be managed by your team.
- **Policy Templates and Customization –** Effective vulnerability scanning of enterprise environments requires use of scanning templates customized for an organization’s unique network and focused on your organization’s own internal requirements.
- **Vulnerability Threat Correlation –** Vulnerability Threat Correlation (VTC) enables organizations to map potential threats to known vulnerabilities that exist in assets in your network and highlighting risks associated with threats that are targeting known vulnerabilities. VTC is only available to NTT Vulnerability Management clients that are also subscribe to Enterprise Security Management and /or Threat Detection services.
- **DHCP Support –** DHCP Support included with the NTT Vulnerability Management service enables organizations to track assets through time, even if their IP address changes.
- **PCI-compliant workflow –** NTT, through its partnership with NTT Security, is an approved Payment Card Industry Approved Scanning Vendor (PCI ASV).

- **Reporting Flexibility –** NTT’s Vulnerability Management service includes customizable vulnerability and remediation reports, as supported by the Qualys Security as a Service (SaaS) Portal, with dozens of available metrics to help organizations measure the performance of their vulnerability management program.
- **Qualys Vulnerability Management –** NTT works with you and will manage and tune the vulnerability management system to ensure false positives and other conditions are filtered out of future reports. As a result, you organization will spend your time remediating vulnerabilities, not digging through repetitive false positive laden reports.

The benefits include:

- **Flexibility** - custom program development, designed for organizational requirements.
- **Enhance the intelligence** – the NTT monitoring program via the Vulnerability Threat Correlation service enhancement helps your analysts by providing up to date and accurate Threat Intelligence.
- **Repeatable and transparent** – processes that integrates and supports your ongoing vulnerability management program.
- **Cost effective** – by leveraging our skilled analysts which may augment or replace staff that lack of internal subject matter expertise for managing a vulnerability management program.
- **Compliant** – through certification and against regulations such as PCI-DSS, HIPAA, and NERC-CIP.
- **Timely** – gain visibility into threats and vulnerabilities across network environment and cloud assets 7X24X365 at your convenience.
- **Transform and execute** – threat and vulnerability data into actionable intelligence to assist in eliminating attack vectors and accelerating remediation.

1.2. Service Matrix

The Vulnerability Management service is offered in three Service Tiers, each consisting of a set of core Service Features, such as the Client Portal and 7X24X365 Security Operation Center (SOC) support. Features and Tiers are listed in Table 1 service matrix below. The Service Tiers, and associated Service Levels are formalized in a Record of Entitlement that forms a part of the client’s Managed Services Agreement.

Feature	Service Tier 1	Service Tier 2	Service PCI Tier
Scan Configuration & Tuning	1	8	1
Scan Scheduling & Maintenance	Yes	Yes	Yes
Standard Reports	3	9	3
Custom Reports	0	2	0
SOC Scan Reviews	0	1	1
On-Demand Scans	0	0	1
Asset Configuration	1	12	1
Discovery Scans & Reports	1	1	1
Authenticated Scanning Support	Yes	Yes	Yes
Qualys Portal SaaS Walkthrough	Yes	Yes	Yes
VTC Support[1]	Yes	Yes	Yes
AWS Support	Yes	Yes	Yes
DHCP Support	Yes	Yes	Yes
Vulnerability Management Support	Yes	Yes	Yes
VM Dashboard	Yes	Yes	Yes
Assigned Service Delivery Manager	Yes	Yes	Yes
24x7x365 SOC Support	Yes	Yes	Yes

Table 1 Service matrix

[1] Vulnerability Threat Correlation (VTC) is available to NTT Vulnerability Management clients that also subscribe to NTT managed security services.

1.3. NTT’s Managed Security Services Portfolio

The NTT portfolio of Managed Security Services help reduce the burden of constant and proactive network monitoring, advanced security analysis, and global intelligence correlation. All our Managed Security Service offerings are powered by the NTT Security platform and combined with NTT's proven combination of people, process and technology.

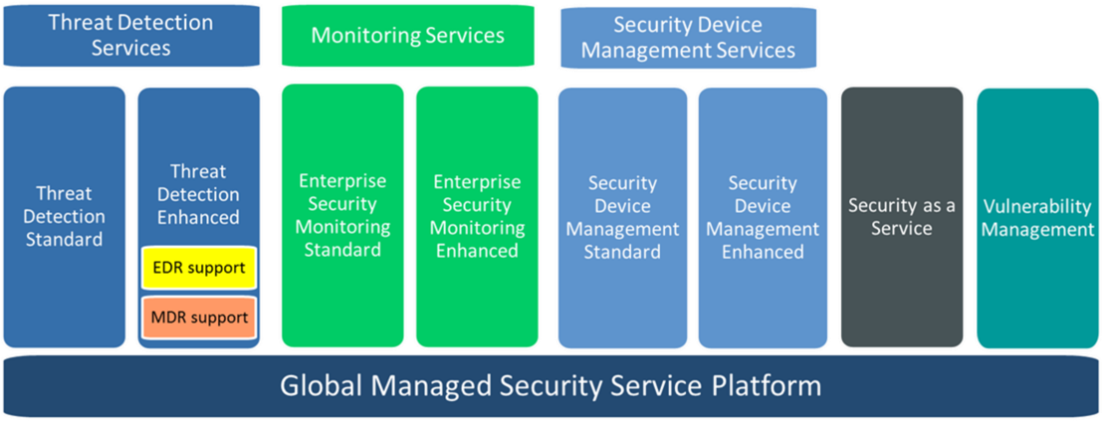

Threat Detection Services
Monitoring Services
Security Device Management Services
Threat Detection Standard
Threat Detection Enhanced
EDR support
MDR support
Enterprise Security Monitoring Standard
Enterprise Security Monitoring Enhanced
Security Device Management Standard
Security Device Management Enhanced
Security as a Service
Vulnerability Management
Global Managed Security Service Platform

Figure 1 – Global Managed Security Service Platform

The portfolio of Managed Security Services consists of:

- **Threat Detection Services.** The Threat Detection Services include Standard and Enhanced services for advanced detection, investigation, and reporting of Security Incidents. The Threat Detection – Enhanced service includes support for Endpoint Detection and Response technologies, as well as Managed Detection and Response capabilities.

- **Monitoring Services.** The Monitoring Services include Standard and Enhanced services for security detection and compliance reporting. The Monitoring – Enhanced service includes support for Endpoint Detection and response technologies. Enterprise Security Program Services (ESPS), which add consulting services for strategic planning, architecture, implementation, reporting, and overall security program guidance can be added to Enhanced monitoring services.

- **Security Device Management Services.** The Security Device Management services include Standard and Enhanced services for management of a broad range of security technologies.

- **Vulnerability Management.** The Vulnerability Management Services deliver customized vulnerability scanning with a variety of compliance and reporting options.

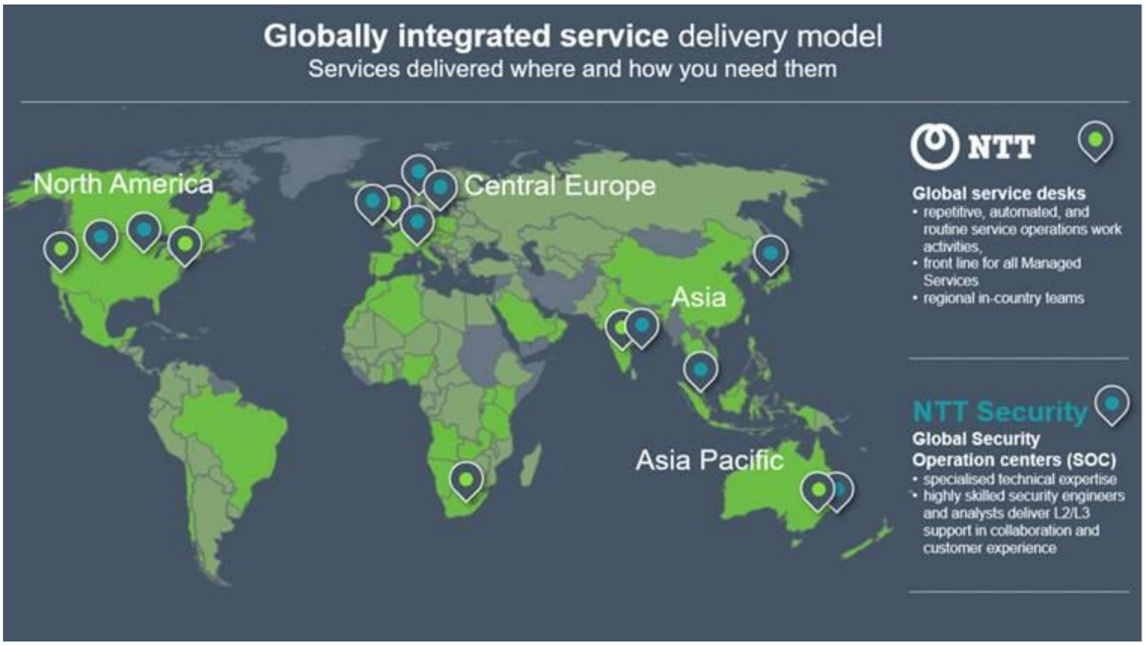
- **Web Security as a Service –** In development.

2. Detailed Service Element Descriptions

2.1. 24/7 Security Operations Center Coverage

Vulnerability Management as a Service is delivered out of multiple Security Operations Centers (SOC) across the globe. These are manned on a 24/7 basis by Security Analysts with extensive vulnerability and threat detection knowledge, and supported by strong technical capabilities of the Global Managed Security Service Platform (GMSSP).

Security Analysts will assist with scan maintenance, troubleshooting, configuration, launching on-demand scans as well as stopping scans, asset maintenance and general service and or reporting questions.



Globally integrated service delivery model

Services delivered where and how you need them

Global service desks

- repetitive, automated, and routine service operations work activities,
- front line for all Managed Services
- regional in-country teams

NTT Security

Global Security Operation centers (SOC)

- specialised technical expertise
- highly skilled security engineers and analysts deliver L2/L3 support in collaboration and customer experience

Figure 2 – Global Delivery Model

2.2. Scan Configuration & Tuning

NTT work with you to configure the appropriate number of Scan Configuration templates based on the Service Tier selected and number of templates defined in the Client Contract. A configuration template is used for a single scan.

For example, if you would like to have one Scan Configuration template for all Desktops, one scan for all assets in a DMZ, one scan for all printers, and one scan for detection of specific Common Vulnerabilities and Exposures (CVEs), that would require four (4) scan configurations.

2.3. Scan Scheduling & Maintenance

NTT manages and maintains all Scan Configuration schedules once deployed.

2.4. Reporting

2.4.1 Standard

The quantity of standard reports available to you via the Security Portal is based on the Service Tier selected. NTT generates reports as defined in the Qualys Vulnerability Management platform. The default reports included in the Vulnerability Management service are described below:

Executive - This report, appropriate for non-technical management, compares vulnerability assessment results over a time period, providing security trend information in summary format. A bar graph shows the number of vulnerabilities by severity, and a flow graph shows the number of vulnerabilities over time. This report includes no detailed vulnerability information.

Technical - This report, appropriate for technicians, displays detailed results from the most recent vulnerability scan. This report includes vulnerability information sorted by host as well as a detailed description of each vulnerability, the recommended solution to remove the vulnerability, when the vulnerability was first and last detected, the consequences if the vulnerability is exploited, as well as the scan test result, where appropriate, showing how Qualys was able to confirm the vulnerability existed, such as the existence or lack of a registry key.

High Severity - This report identifies all severity level 4 and 5 vulnerabilities, the highest severity levels and thus the vulnerabilities that pose the most serious threat to network security. Included in the summary are two graphs, identifying operating systems detected and services detected. Detailed host and vulnerability data, sorted by host, is provided.

Score Card - The Vulnerability Scorecard Report gives you the latest vulnerability status about selected asset groups. By configuring a business risk goal, you can quickly review the comprehensive risk posture of different groups or business units. Additional vulnerability management metrics give managers a way to track remediation efforts.

Patching - The Patch Report identifies hosts that are missing required patches and software. Specify up to 10 QIDs for required patches and 2 QIDs for missing software at run time. Each targeted asset group is listed with the hosts from each group that are missing required patches and software.

Asset-specific reports count as a report against a Service Tier. For example, a separate report to be run for 10 separate assets counts as 10 reports, rather than a single report.

2.4.2 Custom

Custom Reports are available based on Service Tier and must be generated from existing templates within the Qualys portal.[2]

2.5. Asset Configuration

NTT will configure the number of Configuration Items defined by the Service Tier for the purposes of scanning, reporting and remediation. NTT will perform basic maintenance of Asset Configurations at its discretion.

2.6. SOC Scan Reviews

The SOC will perform one hour in depth scan review status calls with you as defined by the selected Service Tier. SOC review calls are not intended to be consultative regarding the Vulnerability Management program design or program guidance. The SOC will review findings, discuss scan results, and discuss general strategies to improve your Vulnerability Management program and or enhance potential reporting initiatives. Vulnerability Management program design and guidance services are available Professional Security Services (PSS).

[1] The Qualys' License agreement prohibits third party modification of reports.

2.7. On-Demand Scans

NTT will perform the number of on demand scans as defined by the Service Tier.

2.8. Authentication Scans

NTT will facilitate the deployment and configuration of Authenticated scan credentials within the Qualys SaaS platform in support of the scan configuration templates.

2.9. Vulnerability Management Support

NTT makes available to you the Qualys Vulnerability Management service workflow management functionality to aid in classification and management of False Positives issues. The SOC will manage the Vulnerability Management system in either a managed or co-managed capacity. For users of the PCI module, workflow is mandated by the portal to align with PCI rules and does not follow standard vulnerability management service rule processes.

2.10. Qualys Web Dashboard

NTT utilizes the Qualys SaaS portal and dashboards for representation and extraction of client data. NTT makes no guarantees as to the accuracy and or content. Qualys reserves the right to change the dashboard and or portal functionality at any time.

2.11. Qualys Portal SaaS Walkthrough

A member of the NTT Vulnerability Scanning Team will conduct a one-hour overview and walk through of the Qualys portal to educate you on standard reporting (Executive & Technical) as well as additional reporting options. This feature is for Tier II clients. An overview of the Asset, Credential, Vulnerability Management functions of the Qualys portal is the focus of this walk through.

2.12. VTC Support

For Vulnerability Management service clients that subscribe to Enterprise Security Management and / or Threat Detections services, all vulnerability scans that are managed and or conducted by NTT will automatically be processed for vulnerability threat correlated log analysis enhancement.

2.13. Qualys License Levels

Qualys Licenses purchased on behalf of a client are dependent on the client specifics and requirements, as well as restrictions therein, as enforced by Qualys and subject to change at any time. License purchased will be detailed in the NTT contract and or SOW.

License	Self Service Scans	Qualys VMS Accounts	Internal Scan Appliances
Enterprise	Unlimited	Unlimited	Unlimited
Express	Unlimited	Unlimited	Max of 5
Scan on Behalf	Not Available Currently	Unlimited Read Only	Unlimited

2.14. Qualys Vulnerability Management System (VMS)

The Qualys VMS supports remediation tracking workflow functions, advanced reporting, and asset management functions delivered in the Qualys self-service portal.

NTT's support of the Qualys VMS is limited to basic functionality and does not include creating or closing Qualys tickets or additional reporting beyond what is defined in the Service Tier. The SOC will maintain the Qualys VMS for NTT Vulnerability Management service clients. This involves opening a ticket in the Qualys VMS for the individual records in question and setting them to Ignored/Closed. This is the only disposition record currently available within Qualys's VMS. If required NTT will create and maintain policies that create tickets in a Closed state for recurring scan issues.

3. Vulnerability Service Process Overview

The Vulnerability service process includes, but is not limited to, capturing information of the client's service requirements, SLAs, Configuration Items, site and contact details, configuration of connectivity and the implementation and activation of the Manage Centre portal and Security portals.

NTT utilizes a multi-phased approach to coordinate and perform the scanning service:

- Optional Vulnerability Management Program Design PSS Services are available for Complex and Enterprise scale engagements.
- Phase 1 - Scanning Configuration
- Phase 2 – Vulnerability Discovery and Processing
- Phase 3 – Scanning Results and Reporting.

NTT provides you with access to the Security Portal and supports accessing standard and subscribed reports for the scanning service. NTT assigns an Account Team to work with you throughout the performance of Services and may consist of one or more of the following: Service Delivery Manager (SDM), Information Security Engineer (ISE).

NTT will provide a URL and initial logon credentials to your point of contact for access to the Security Portal, as well as online training. NTT will supply you with a minimum of one read only account into the Qualys Portal for Report and Vulnerability Management Functionality. Administrative scan functionality is dependent on the license level selected. NTT's SDM will work with your point of contact (POC) to complete the services questionnaire, which details your 'in-scope' IPs and escalation procedures. If NTT is contracted to provide more in-depth vulnerability management consultative services, we will work with you to complete aforementioned questionnaire.

3.1. Phase 1 – Scanning Configuration

Discovery Scans are not required but may be run at the start of each assessment window depending on Service Tier selected. NTT reserves the right to run Discovery Scans at the SOC's discretion. The SOC uses Discovery Scans to help validate scope and license(s), or other concerns the client or the SOC may have before an assessment starts.

Note: Discovery scans reports are based on a single cumulative report.

NTT configures the Qualys scanning system with the appropriate IPs and scan configurations as defined by your Service Tier. The SOC will schedule the scan start time per your direction. All scans run until completion and may not be paused.

If an estimate on scan time is required, please create a Service Request with the SOC.

3.1.1 Asset Tag Configuration

Host asset tag configuration is limited to the number defined by the selected Service Tier and or contracted for in the client specific contract and or SOW. NTT will configure and maintain the designated allotment of Configuration Item within the Qualys SaaS platform typically using either a client provided configuration item list or subnet range definition provided via the on boarding questionnaire.

3.1.2 DHCP Support

DHCP system support must be configured at the beginning of all scan engagements. Discovery scans of DHCP configurations are conducted at the discretion of the SOC. Changes to the DHCP tracking mechanism is an element of Qualys' scanning system and not the responsibility of NTT. Changing DHCP support models after a scan has been completed could, dependent on the type of changes being made, result in a loss of accumulated historical scan data.

3.2. Phase 2 – Vulnerability Discovery and Processing

NTT scans network devices to identify potential vulnerabilities. Detection of vulnerabilities is based on specific scan settings among other factors. For a detailed description of Host and Vulnerability detection procedures please contact your SDM.

Information collected during this phase includes, but is not limited to, the following:

- Open / Closed Port detection
- Service type and version fingerprinting
- Service Interrogation for vulnerabilities
- Rudimentary Application Form / Variable Interrogation
- Operating System (OS) identification

NTT reserves the right to manually validate and investigate vulnerability results, per NTT's QA process.

3.3. Phase 3 – Scanning Results and Reporting

The Vulnerability Management service utilizes the Qualys SaaS platform to generate all reports. All standard and set reports are delivered through the Security Portal.

Report deliverables are defined by the Service Tier.

Scanning review and service delivery calls are performed as defined by the Service Tier.

NTT SOC support is available 24/7 for technical questions via email or telephone.

SOC Support is available to aid, investigate and troubleshoot scan issues, assist with access to the vulnerability management systems, starting and stopping scans and general vulnerability management service questions.

3.3.1 On-Demand Scans

You can request On-Demand scans, which are subject to the Service Tier selected as well as the following conditions. The Client requesting On-Demand scans must submit an On-Demand scan request via the SOC at least 24 hours prior to the required start time. Requests must include an authorized scan window and be directed from an authorized employee within your organization.

3.3.2 Service Requirements

Client will assign a POC to complete a services questionnaire, approve scanning configuration, and communicate with NTT sales executives as needed for follow-up and problem resolution.

Client owns, manages, and controls the IP Address Range(s), Internet-accessible IPs, and Internet-accessible devices considered 'in-scope'.

3.3.3 Self Service Scan Support

Clients with Enterprise or Express licenses can perform unlimited self-service on-demand scans of in scope IP's.

3.4. PCI ASV Service Requirements

Client must follow each payment card organization's respective compliance reporting requirements to ensure compliance. While scan reports must follow a common format, the results must be submitted according to each payment card organization's requirements. Contact the client's acquiring bank or check each payment card organization's regional web site to determine to whom results should be submitted.

PCI reporting occurs on a quarterly basis.

NTT publishes the PCI report to the Portal.

The PCI report describes the type of vulnerability or risk, a diagnosis of the associated issues, and guidance on how to fix or patch the isolated vulnerabilities.

For PCI ASV scanning, clients are required to white list NTT Security and Qualys scan ranges through their DMZ in accordance with PCI ASV Program Guideline rules. Please see the PCI website: https://www.pcisecuritystandards.org/ or contact the client's SDM for the latest requirements.

If the client utilizes IPS auto-shunning technology, proxy firewalls (or similar technologies), the client must implement one of the following to ensure NTT can produce accurate scanning results:

- Appropriately configure router Access Control Lists (preferred method)
- Configure devices to monitor and log, but not block NTT Security's incoming IPs
- Interface filters directly on the firewall, Disable this feature for NTT Security's scanning IP(s).

Should the client need to substitute 'in-scope' IPs, the client agrees in good faith to work with NTT to amend the scope of work accordingly.

If load balancing is in use, the client must provide NTT with written assurance that the infrastructure behind the load balancers is synchronized in terms of configuration Note: If the client fails to provide written assurance, PCI Security Standards Council requirements state NTT must individually scan the components from an internal location within the client's environment. If internal scanning is required, NTT will work with the client to amend the scope of work accordingly.

If client elects to receive ASV PCI Services client agrees to be bound by the terms and conditions of the then current version of the PCI DSS Validation Requirements for ASVs (visit the PCI Security Standards Council website for more information: https://www.pcisecuritystandards.org/) set forth by PCI Security Standards Council.

4. Our Approach to Service Operations

4.1. Service Experience

NTT's desire is to maximize the value you receive from Managed Security Services through effective engagement, communication and information sharing. Our focus is to enhance your service experience and provide your organization with insight – to enable your business decisions.

4.2. Service Desk

NTT's regional Managed Service Centre (MSC) is your primary Service interface, available to you 24/7/365. The NTT MSC coordinates incidents, and service requests, as well as system administration functions. They interact with you from a Service contract perspective, and as such, will have access to contract details, service information (service entitlements), site data and contact information, site and network diagrams, and configuration item/IT service data. They also ensure the knowledge management system is updated and kept current for your network infrastructure, action any service requests.

The service desk logs, tracks, and closes all tickets (incidents and service requests) in the NTT service management system. Tickets can be logged through the following methods:

- event driven (through monitoring of the environment)
- directly reported to NTT by you through the service desk
- directly reported to NTT by you via the Manage Centre portal
- directly reported by NTT Security via our Integrated Service Desk

When contacted by you, the MSC will manage your contact through to resolution, including:

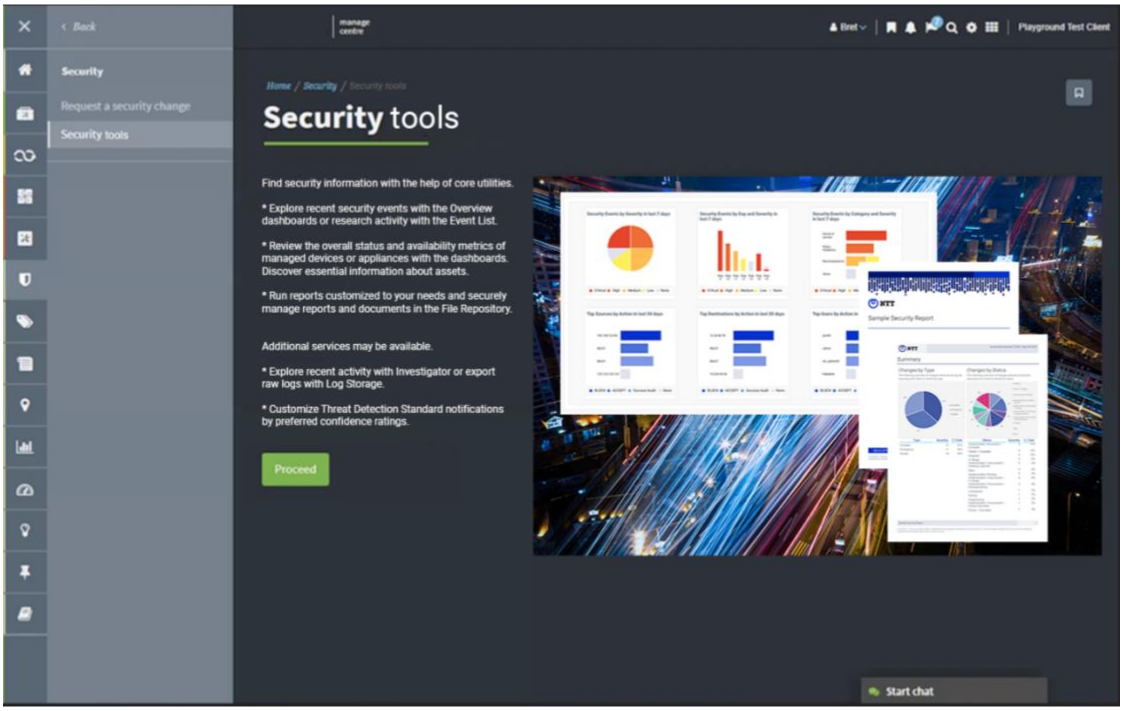
- initial classification and prioritization
- assignment to correct resolver group
- ticket updates
- closure once resolved/completed or as contracted

4.2.1 Manage Centre Portal

As part of any Managed Security service, you are provided with access to NTT's Manage Centre portal. Manage Centre provides online access to:

- Interact with NTT's online logging of incidents, requests and changes.
- Track, view and submit comments within incidents, requests, change and problem tickets.
- View contract data.
- Browse and search NTT's knowledge base.

- Access the online document repository – e.g. for contractual documentation, procedural documentation, meeting minutes.



Security tools

Find security information with the help of core utilities.

* Explore recent security events with the Overview dashboards or research activity with the Event List.

* Review the overall status and availability metrics of managed devices or appliances with the dashboards. Discover essential information about assets.

* Run reports customized to your needs and securely manage reports and documents in the File Repository.

Additional services may be available.

* Explore recent activity with Investigator or export raw logs with Log Storage.

* Customize Threat Detection Standard notifications by preferred confidence ratings.

Figure 3 – Manage Centre Portal

4.2.2 Online Dashboards and Charts [3]

Reporting is provided via NTT's Manage Centre portal, through a mixture of interactive dashboards, charts and downloadable reports. Through Manage Centre, users can:

- View summaries and drill down into the detail for analysis.
- Focus in on specific time periods.
- Apply a range of filters e.g. location, technology class, make/model, priorities, status, root cause, etc.
- Export the underlying data for offline analysis or reformatting.

Interactive reporting is available for:

- service levels
- task-related data e.g. incidents, problems, requests, changes
- service assets and configuration items
- availability, capacity and performance data

Dashboards and charts are provided through four functions within the portal:

- Interactive charts – provides a range of configuration item (CI), task, availability and performance charts with ability to group, filter and drill into the details.
- Dashboards – summary snapshots for specific views of information about your environment e.g. service levels, device health, and asset details. These also enable you to drill into the details.
- CI-Specific charts – when you are viewing a specific infrastructure configuration item, you also have the option to drill into task, availability and performance charts specific to that CI.
- Library – the library provides a document repository where electronic documentation and reports are stored for viewing and download.

4.2.3 Omni-channel Communications

NTT utilizes omni-channel technologies to provide you with a variety of ways to communicate with NTT for a seamless experience:

- Telephone
- Email
- Manage Centre Portal

Omni-channel technology enables the context of discussions to be identified, to streamline communications between the user and NTT staff, and to avoid the need for repetitive explanations.

Our omni-channel platform interfaces with our ITSM system to ensure all interactions are captured and appropriate ticketing is auto-created and updated for tracking and analysis.

4.3. Client Security Portal

This portal provides clients with an interface specific to NTT services. The Security Portal delivers multiple levels of security and compliance information to support client management, business and technical needs.

The Security portal features include:

- Event Manager – Complex, granular views to identify, research and mitigate security events.
- Customizable features to tailor analysis and responses to client needs.
- Full-featured reporting with on-demand security, compliance and audit reporting.
- An integrated document management system.
- Built-in third-party ticket system integration via a REST API.
- Pre-determined client user accounts and easy to access documentation.

This section discusses features of the Client Security Portal.

4.3.1 Event Manager

One of the key functional areas of the Client Security Portal is the Event Manager, which allows users to view and address events impacting their environment in real time.

4.3.2 Event Summary

After clicking on an event from within the Event Manager menu, Portal users access the Event Summary page.

The Event Summary page is designed to provide a detailed understanding of the activities that generated an event and the potential impact of those activities. The Security Portal provides detailed information, such as IP addresses, detection methods and historical summaries that enable clients to rapidly determine the source of the activity and potential risk to their environment.

Individual events provide tools relevant to each issue, allowing users to research and manage them by:

- Grouping details by type, hosts and timing.
- Viewing risk information such as score or kill chain stage.
- Viewing geographical, list or asset information.
- Viewing correlated events and raw log details.

5. Our Approach to Service Transition

The NTT Transition approach aims to ensure that both organizations enter the transition with a clear idea and understanding of the goals and objectives of the transition.

5.1. Objectives of Service Transition

- To ensure the absolute minimal business disruption during the transition of the managed service.
- To facilitate a smooth and trouble-free transition.
- To determine and manage realistic transition timeframes.
- To establish an operational baseline for the global managed services delivery organization that will be responsible for delivering the service post-transition.
- To facilitate and conclude the contracting process.
- To develop and build a sound business relationship from the onset.
- To align your expectations with service delivery capabilities and constraints.
- To ensure our people understand your business from the onset to deliver reliable, stable and excellent service.

5.2. Transition Methodology

NTT uses a formal transition methodology, called the Transition Implementation Methodology (TIM), developed in-house from industry-leading best practices and years of practical experience with the transition of operations from its clients and/or incumbent service providers. It is a formal methodology that allows flexibility for adjustment to cater for a wide spectrum of operational services, assets, staff, policies, process, standards and architectures to be transferred to NTT. We see three common scenarios with client transitions:

- Existing clients who have been utilizing NTT's Support Services and have decided to commence the journey into Managed Services.
- Existing clients who originally requested a bespoke outsourcing construct in the past, but are now wishing to take advantage of standardized, optimized and automated operations service.
- New clients joining NTT to take advantage of our managed services offerings.

Our transition methodology caters for all these scenarios and provides us with the flexibility to bring your IT environment under the operations of our Managed Services in a seamless manner.

TIM recommends that the transition project is planned and executed over five phases – Inception, Definition, Build, Deployment and Close. Each phase has clearly defined activities, deliverables and accountabilities, described later in this section.

The following diagram outlines the TIM process and how it interrelates to our Service Activation Process:

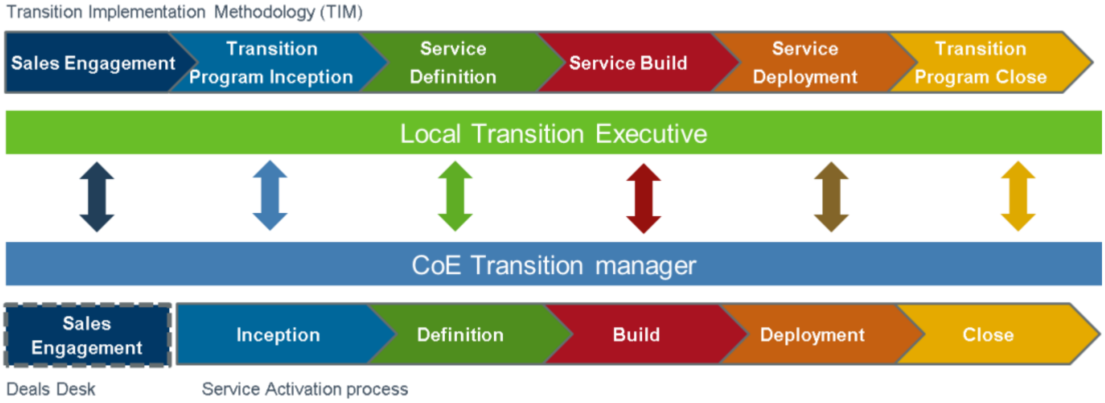


Figure 4: Transition Implementation Methodology and Service Activation Process

NTT's local Service Transition Manager is responsible for managing the transition process with you and your organization following TIM, and coordinating back with our Center of Excellence (COE) Transition Team. The COE Transition Team is responsible for running the service activation process to enable our service operations. As part of the service activation process, the tools and systems are setup and activated for the managed service to go live.

The typical duration for service transition is 12 weeks, although timing will depend on the size and complexity of the environment.

Our methodology is supported by a suite of transition tools to enable us to optimize activation of our service into your network environment:

- Auto-discovery tools that enable NTT to validate and enrich your asset listings as we populate your environment into our CMDB.
- Automated deployment tools to build the monitoring and management domain within our Managed Services Platform specific to your network environment and to commence monitoring activities.
- Pre-defined monitoring plans to establish the event criteria most appropriate for monitoring the CIs within your network environment, and with the ability to tune thresholds based on your needs.

5.3. Service Transition Phases in Detail

The following sub sections provide more detail of NTT's Transition Phases, as summarized in Figure 4 above:

5.3.1 Sales Engagement Phase

The following high-level activities will be performed during this phase and are typically those activities we perform before the Transition Commencement Date and Contract Signature.

- **Due diligence.** The objective of the Due Diligence is to verify all information received, confirm solution and pricing proposed, and to collect sufficient information to complete the detail transition planning.
- **Contract negotiations:** Define, negotiate and agree all legal agreements between you and NTT. This includes service schedules, definitions and commercial terms.
- **Detail transition planning:** The initial phase of the NTT transition project is the planning and preparation phase. The success of the transition relies heavily on the time and effort spent on various assessments, implementation of transition governance, and ultimately detailed planning.

5.3.2 Inception Phase

The Inception phase is where we kick-off the transition and engage the required stakeholders.

The Transition manager will conduct the kick-off workshop with you to understand the transition requirements and then with internal teams for the sales handover and drafting the transition plan.

The asset list of your network infrastructure is reconciled with device information scanned by our auto-discovery tool, to produce the Configuration Management Database (CMDB). The CMDB will feed our monitoring, service management and billing systems with the required device information.

5.3.3 Definition Phase

During the Definition phase, the transition timelines and the infrastructure design is reviewed and agreed with you. Design of the connectivity to your network environment is also completed in this phase.

Configuration of the Managed Services Platform is initiated for activation of the service.

5.3.4 Build Phase

The Build phase covers the monitoring and management tool activation, along with establishing connectivity to your network. Configuration Items are loaded into the monitoring tools using auto-deployment systems where possible, and thresholds e.g. capacity are configured for event monitoring.

A standard Service Operations Manuals is created, and knowledge articles are created, reviewed and loaded into the ITSM system.

Omni-channel communication configuration is setup during this phase.

5.3.5 Deployment Phase

During the Deployment phase, knowledge transfer sessions are held with you, your incumbent provider (if applicable) and implementation teams. You are provided with training materials and any necessary training sessions are scheduled, including familiarization with our portals.

Operational Readiness Testing is completed and signed off prior to Service Go-Live. Service Go-live communications and welcome pack are also shared.

5.3.6 Close Phase

The objective of the Closure phase is to ensure the managed service is stable and delivering as per agreement, implement corrective actions, complete final operational documentation, and to formally close the service transition.

Activities during this phase include:

- Ensuring all documentation is updated and stored safely.
- Documenting lessons learned from a Post-Transition review.
- Your sign-off on completion of the transition.

6. Service Management

6.1. Service Level Management

Depending on the complexity and/or size of your environment, the mix of products and services, NTT may recommend additional Service Delivery Management options.

6.1.1 NTT Service Delivery Manager (SDM)

Service Delivery Management provides governance and control across the various service features, processes, and systems necessary to manage the full lifecycle of the Security Device Management services.

NTT assigns a Service Delivery Manager (SDM) to be responsible for Service Level management, and to act as an advocate for your organization within NTT. The NTT SDM is the primary interface who will manage the S ervice Delivery relationship between your organization and NTT. The SDM is responsible for scheduling, running all service management review meetings, and ensures all processes and documentation are in place to manage your services.

Deliverables of the NTT SDM include:

- Establish client relationship.
- Capturing and managing minutes, agenda items, actions, and decisions.
- Change Management Issue Management.
- Escalation Management.
- Risk Management.
- Service level monitoring, reporting and management.
- Service review meeting.
- Work with Service Transition Teams.

6.1.2 Technical Account Manager (TAM) - Optional

The Technical Account Manager (TAM) is an Optional resource that provides overall account management and specialized technical support to you by responding to action items, emails, and customer calls, and by proactively initiating actions to ensure client satisfaction. The TAM is the point of contact for Incidents and Service Requests that are outside the scope of support provided by the Support Operations Center (SOC). The TAM also manages designated accounts both by responding to technical questions, issues, and opportunities; as well as by overall management of requests and general account satisfaction levels. This position is primarily technical in nature, with a high level of customer interface, and requires strong prioritization and project skills.

6.1.3 Incident management

Incident management is the process for managing the lifecycle of an Incident. The aim is to restore the Threat Detection service as quickly as possible to minimize business impact. This is achieved through a temporary workaround or permanent fix, within the Service Level targets.

As part of the Threat Detection service, we proactively identify incidents on Configuration Items. NTT or NTT Security notifies you within 15 minutes of the incident. The 15 minutes begins when the incident, indicating a change of state is received by NTT’s monitoring system.

The Incident management process includes notification, status update, and escalation procedures that are executed by the NTT Service Delivery teams on a 24/7/365 basis.

6.2. Change Management Support

NTT partners with your Change Advisory Board (CAB) to support Changes to your environment. Standard Change requests can be made via the Manage Centre portal, or Service Requests logged to the NTT MSC. More specifically, you can request Moves, Adds, Changes, Deletions (MACDs) to your Configuration Items and for minor configuration Changes that have been pre-approved by your CAB as Standard Changes.

6.2.1 Change request management

NTT manages Requests for Changes (RFCs) on your behalf through the Change lifecycle. This includes the following:

- providing a method for logging RFCs
- classifying and managing Change in accordance with its classification:
  - standard (pre-approved) Changes
  - normal Changes
  - urgent Changes
  - Emergency Changes
- requesting an impact analysis to be completed by the appropriate client stakeholders
- distributing relevant documentation for review prior to CAB meetings.

Appendix A Service Level Agreements

Category	Description	Priority	SLA	Service Credits	Service Credit Limit	Service Calendar
Request Response	NTT will assign a Service Request with priority ____ within ____ minutes of receiving the ticket at NTT`s Service Desk.	P1&P2	60 Mins	5% of Monthly Service Fee	N/A	N/A
		P3&P4	4 Hours			
Request Complete	NTT will resolve a Service Request with priority ____ within ____ minutes of receiving the ticket at NTT`s Service Desk. .	P1	2 Business days	95% Service Units of the Request	95% Service Units of the Request	N/A
		P2&P3	5 Business days			
		P4	10 Business days			

Table 2 – Service Level Agreements

Appendix B

Appendix C Qualys License Level and VMS

Qualys License Levels

Qualys Licenses purchased on behalf of a client are dependent on the client specifics and requirements as well as restriction therein as enforced by Qualys and subject to change at any time. License purchased will be detailed in the NTT contract and or SOW.

License	Self Service Scans	Qualys VMS Accounts	Internal Scan Appliances
Enterprise	Unlimited	Unlimited	Unlimited
Express	Unlimited	Unlimited	Max of 5
Scan on Behalf	Not Available Currently	Unlimited Read Only	Unlimited

Qualys Vulnerability Management System (VMS)

The Qualys VMS supports remediation tracking workflow functions, advanced reporting, and asset management functions delivered in the Qualys self-service portal.

NTT’s support of the Qualys VMS is limited to basic functionality and does not include creating or closing Qualys tickets or additional reporting beyond what is defined in the Service Tier. The SOC will maintain the Qualys VMS for NTT Vulnerability Management service clients. This involves opening a ticket in the Qualys VMS for the individual records in question and setting them to Ignored/Closed. This is the only disposition record currently available within Qualys’s VMS. If required NTT will create and maintain policies that create tickets in a Closed state for recurring scan issues.