SERVICE DESCRIPTION

Managed External/Internal Vulnerability Scanning

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

Contents

1 Service Prerequisites

1.1 General Requirements

1.1.1 Service Selection

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

1.1.2 Address Ownership

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

1.1.3 Client Point of Contact

Client will assign a main Point of Contact (POC) to work with NTT Ltd.'s 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 NTT Ltd.'s Client Security Service Detail (CSSD) form.
- Client's 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.

1.1.4 Access and Connectivity

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

1.1.5 Client Staff and Resources Requirements

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

- Notifying NTT Ltd. of any potential problem areas, which could interfere with scanning activities, such as load-balancing.
- Resolving Internet Service Provider (ISP) outages and internal network infrastructure issues.
- Ensuring information provided to NTT Ltd. is accurate (e.g., web site banners, hardware, software, OS, application versions, etc.) for NTT Ltd. to properly validate vulnerabilities for PCI ASV dispute resolution.
- Notifying NTT Ltd. of any new devices substituted into 'in scope' IP address ranges.

1.1.6 Change requests

If Client wants to request changes to any managed scan configuration defined within a specific service tier they must notify the NTT Ltd. SOC 24 hours prior to the scan start.

1.1.7 Technologies that may impede delivery

Disabling IP address shunning to ensure NTT Ltd.'s incoming scanning activities will not be affected.

1.1.8 Third-Party Vendors

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

1.1.9 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 agreed by NTT Ltd..

1.1.10 Software Modification

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

1.1.11 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.

1.1.12 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.

1.1.13 Internet Service Provider or Client Network Outages

NTT Ltd. is not responsible for resolving Client's Internet Service Provider (ISP) outages, or issues with Client's internal network infrastructure.

1.1.14 System Backups

NTT Ltd. recommends that Client perform full back-ups of relevant systems prior to the performance of services.

1.1.15 Closure of Alerts and Security Incidents

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

1.1.16 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.

1.2 PCI ASV Service Requirements

1.2.1 PCI Service Consent

If Client elects to receive Approved Scanning Vendor (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 set forth by PCI Security Standards Council (visit the PCI Security Standards Council website for more information: https://www.pcisecuritystandards.org/).

1.2.2 Reporting requirements

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

1.2.3 Reporting frequency

PCI reporting occurs on a quarterly basis.

1.2.3.1 NTT Ltd. publishes the PCI report to the Portal.

1.2.3.2 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.

1.2.3.3 For PCI ASV scanning, Clients are required to white list NTT Ltd. and Qualys scan ranges through their DMZ in accordance with the then current PCI ASV Program Guideline rules. Please see the PCI website: https://www.pcisecuritystandards.org/ or contact your SDM for the latest requirements.

1.2.3.4 If Client utilizes IPS auto-shunning technology, proxy firewalls such as VelociRaptor®, defense mechanisms such as SynDefender®, or the PIX® TCP Intercept feature (or similar technologies), Client must implement one of the following to ensure NTT Ltd. can produce accurate scanning results:

Appropriately configure router Access Control Lists (preferred method)

- Configure devices to monitor and log, but not block NTT Ltd.'s incoming IPs
- Interface filters directly on the firewall
- Disable this feature for NTT Ltd.'s scanning IP(s)

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

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

1.2.3.7 For PCI ASV scanning services Clients are required to adhere to and follow the Qualys PCI Portal based workflow process.

2 Core Service Elements

2.1 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.

2.2 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 platform locations unless there is prior agreement and approval between NTT Ltd. and the Client.

2.3 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.

2.4 Language support

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

3 Service Features

3.1 Service Components

Features of the NTT Ltd. Vulnerability Management service include the following, and depend on purchased scope of services.

- **External and Internal Scanning Options –** External vulnerability scanning specifically examines an organization's security profile from the perspective of an external outsider. External vulnerability scanning helps an organization identify and remediate vulnerabilities within their IT environment before they potentially use the vulnerabilities to access, modify or destroy confidential information. Internal vulnerability scanning operates inside your business's firewall(s) to identify real and potential vulnerabilities inside your business network.
- **Managed or Self-Service Scanning –** NTT Ltd. VM offers flexibility in scan management – scans can be managed and executed by expert analysts in NTT Ltd. operation centers, or can be Client managed and executed.
- **Policy Templates and Customization –** Effective vulnerability scanning of enterprise environments requires use of scanning templates customized for the organizations unique environment and centered around scanning work plans tailored to each organization's own internal processes.
- **Vulnerability Correlation –** Vulnerability Correlation enables organizations to map potential threats to known vulnerabilities that exist in assets in the environment, highlighting risks associated with threats that are targeting known vulnerabilities. NTT Ltd. supports a four-tiered vulnerability logic process to

provide analysts and Clients with an accurate threat mapping to best act in response to the data in real time. Vulnerability Correlation is available to NTT Ltd. VM Clients that are also Clients of the Threat Detection – Enhanced.

- **DHCP Support –** DHCP Support included with the NTT Ltd. VM enables organizations to track assets through time, even if their IP address changes.
- **Ticket System Integration –** Outputs from the NTT Ltd. VM can be integrated into most modern ticketing systems via a REST API, to enable Clients to utilize their in-house tracking and workflow processes.
- **PCI-compliant workflow –** NTT Ltd. is an approved Payment Card Industry Approved Scanning Vendor (PCI ASV) and as such can provide Clients with a seamless end to end platform for all vulnerability management scanning needs.
- **Reporting Flexibility –** NTT Ltd. VMaaS includes customizable vulnerability and remediation reports as supported by the Qualys SaaS Portal, with dozens of available metrics to help organizations measure the performance of their vulnerability management program.
- **Qualys Vulnerability Management –** NTT Ltd. works with Clients and will manage and tune the vulnerability management system to ensure false positives and other conditions are filtered out of future reports to ensure that Clients spend time remediating vulnerabilities, not digging through repetitive noise based reports.

3.2 Qualys VMS Platform

NTT Ltd. conducts and/or coordinates all Services from a Security Operations Center (SOC) and utilizes the Qualys Vulnerability Management System Platform.

3.3 Service Tiers and Features

NTT Ltd. offers Qualys scanning services through a combination of Service Tiers, license levels, scan frequencies, and optional services, which determines the service features available to Client as described below. The service packages are formalized within Purchase Orders.

The Service tiers are presented in the following table:

Feature	Tier 1	Tier 2	PCI
Feature Tier 1 Tier 2 PCI Scan Configurations	1	8	1
Standard Reports	3	9	3
Custom Reports	0	2	0
SOC Scan Reviews	0	1	1
On-Demand Scans	0	0	1
Pre-Configured Assets	1	12	1
Discovery Scans & Report	1	1	1

3.3.1 Scan Configuration

NTT Ltd. will work with Client to set up Scan Configurations based on the Service Tier selected.

3.3.2 Standard Reports

The quantity of standard reports available to Client via the NTT Ltd. Portal (the Portal) is based on the Service Tier selected. NTT Ltd. generates reports as defined in the Qualys VM platform.

Default reports included are as follows:

- Executive
- Technical
- High Severity
- Score Card
- Patching

Asset-specific reports count as a report against a Service Tier. For example, if Client requires a Technical report to be run for 10 distinct assets, it counts as 10 reports, rather than a single report.

3.3.3 Custom Reports

Custom Reports are available based on Service Tier selected and must be generated from existing templates within Qualys' VM. Qualys' License agreement prohibits third party modification of reports.

3.3.4 SOC Scan Reviews

The SOC will perform one hour in depth scan review status calls with Client as defined by the selected Service Tier. SOC review calls are not intended to be consultative regarding VM program design or program guidance. VM design and guidance services are available via NTT Ltd.'s Consulting Services team. Standard 24x7 SOC Support will assist with scan maintenance, troubleshooting, configuration, results and general reporting questions.

3.3.5 On-Demand Scans

NTT Ltd. will perform the number of On-Demand scans as defined by the Service Tier.

3.3.6 Asset Configuration

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

3.4 Qualys VMS

The VMS supports remediation tracking workflow functions, advanced reporting, and asset management functions delivered in a self-service portal. NTT Ltd.'s support of the Qualys VMS does not include creating or closing tickets or additional reporting beyond what is defined in the Service Tier.

4 Service Delivery Process

4.1 Service Delivery Overview

4.1.1 Service Delivery Phases

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

- Optional VM Design PSS Services
- Phase 1 - Scanning Configuration
- Phase 2 – Vulnerability Discovery and Processing
- Phase 3 – Scanning Results and Reporting

4.1.2 Portal Access

NTT Ltd. provides Client access to the NTT Ltd. Portal and supports accessing standard and subscribed reports for the scanning service. NTT Ltd. will provide a URL and initial logon credentials to Client's POC for access to the Security and Compliance Portal, as well as online training.

NTT Ltd. will provide Client subscribing to Enterprise Scanning services a minimum of one read only account into the Qualys Portal for Report and Vulnerability Management Functionality. Client subscribing to 'On Behalf Of' services will not have access to Qualys Portal.

4.1.3 Account Team

NTT Ltd. assigns an Account Team to work with Client throughout the performance of Services. A member of the NTT Ltd. Account Team will work with Client's main POC to complete the services questionnaire, which details Client's 'in-scope' IPs and escalation procedures.

4.2 Phase 1 – Scanning Configuration

4.2.1 Discovery Scans

Discovery Scans are not required but may be run at the start of each assessment window depending on Service Tier selected. NTT Ltd. 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 Client or the SOC may have before an assessment starts.

4.2.2 Scanning Configuration

NTT Ltd. configures the Qualys scanning system with the appropriate IPs and Scan Configurations as defined by Client's Service Tier. The SOC will schedule the scan start time per Client Service Profile (CSP). All scans run until completion.

4.2.3 Asset Configuration

Asset configuration is limited to the number defined by the selected Service Tier.

4.2.4 DHCP System Support

DHCP system support is configured at the beginning of all scan engagements. Discovery scans for DHCP configuration 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 the NTT Ltd.

4.3 Phase 2 – Vulnerability Discovery and Processing

4.3.1 Vulnerability Discovery

NTT Ltd. scans network devices to identify potential vulnerabilities. Detection of vulnerabilities is based on specific scan settings among other factors. A detailed description of Host and Vulnerability detection procedures can be provided by NTT Ltd. upon request. 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

4.3.2 Validation and investigation

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

4.4 Phase 3 – Scanning Results and Reporting

4.4.1 Reporting Delivery

NTT Ltd. utilizes the Qualys SaaS platform to generate all reports. All standard and set reports are delivered through the NTT Ltd. Portal.

4.4.2 Reporting Deliverables

Report deliverables are defined by the Service Tier.

4.4.3 Scanning Review and Service Delivery calls

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

4.4.4 SOC Support

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 VMS, starting and stopping scans and general VMS questions.

4.4.5 On-Demand Scans

Client can request On-Demand scans, which are subject the Service Tier selected as well as the following conditions. Clients with Enterprise or Express licenses can perform unlimited self-service on-demand scans.

- Client must submit an On-Demand scan request via the SOC at least 24 hours prior to the required start time
- Request must include an authorized scan window

5 Operating Level Agreements

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

6 Changes in Service

6.1 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.

6.2 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.

6.3 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 implementation process, and Classifiers or LTAs may require modification or development.

7 Service Disclaimers

7.1 Qualys License Enforcement

License enforcement within Qualys by NTT Ltd. is by default lifted to allow easier scan configuration and a reduced work load versus the license enforcement mechanism. NTT Ltd. will monitor license quantities and regularly communicate these to Client; however, NTT Ltd. is not responsible for overages. Any overages at the end of the standard yearly contract cycle will be billed to Client at the set per IP rate of their current contract.

7.2 Service Scoping

NTT Ltd. contracts with Qualys and purchases licenses on Clients behalf using many metrics, such as quantity of IP's to be scanned, employee count of the company, desired functionality (internal vs external), physical/virtual appliance architecture, etc. It is the sole responsibility of Client to provide accurate scoping information to NTT Ltd.. If it is determined later an incorrect license was attributed to Client based on inaccurate information, it will be Client's sole responsibility for any billing charges which could occur.

7.3 License True Up Activities

License true up activities and any data purges as a result is not responsibility of NTT Ltd. and a function of the Qualys SaaS portal.

7.4 Qualys Service Outages

Service outages on behalf Qualys are not the responsibility of NTT Ltd..

7.5 Unused IP Address Licenses

Any unused IP licenses at the term of the contract are not refundable.

7.6 IP Address Rotation

Qualys VM IP quantities are licensed and used based on unique visible IPs and or FQDNs seen during vulnerability scans. IPs cannot be rotated during the contract term.

7.7 Solution Recommendations

Solution recommendations are those of Qualys alone and are performed at the discretion and risk of Client. NTT Ltd. is not responsible for damages resulting from Qualys' solution recommendations and suggests that all systems have proper backups prior to implementing any remediation.

7.8 Liability

Client understands and will not hold NTT Ltd. liable for damages because of any Internal, External, or Agent based Qualys scan. Client acknowledges scanning may be disruptive to an environment and could result in Denial of Service, data and or system corruption, loss of data, system crashes or the general performance and availability of systems.

7.9 Identification of Vulnerabilities and False Positives

Client acknowledges that Qualys does not guarantee to find all vulnerabilities, does not perform Web Application assessments and does not guarantee the existence of False Positives.

8 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.

9 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.

- 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.

Together we do great things