Enhanced Security Services - Vulnerability Management as a Service (VMaaS)

1 Overview of the Service

NTT's Vulnerability Management as a Service (VMaaS) is a service that utilizes NTT's' Vulnerability Scanning platform for detecting vulnerabilities in a range of systems in an effort to assist the Client with effective remediation.

NTT's Vulnerability Scanning platform may require one or more of the following Technology configurations:

(a) Internal scanner

(b) External scanner

(c) Agent software

(d) Gateway server software

NTT will deploy the above Technology Configurations as required and necessary to deliver the Service as specified in the SOW.

This service is only available if the Client has contracted in scope one or more of the following NTT Services:

(e) NTT Managed Detection and Response

(f) NTT Managed Cloud Services

(g) NTT Endpoint Management

(h) NTT Managed Networking

2 Client Responsibilities

(a) Provide the necessary assurance and permissions that scans may be conducted by NTT as agreed in the SOW.

(b) Client warrants that it has obtained all consents necessary for the data to be collected and used on its behalf for the End User Endpoint Vulnerability Scanning and that it has a legal basis for requesting such information.

(c) Provide patch management schedule.

(d) Identify any non-standard reporting requirements prior to the service start (parameters, periods etc.)

(e) Provide service account(s) for unmanaged servers/devices for the purpose of authenticated scans.

(f) Provide details of all unmanaged IP spaces where scans will be conducted.

(g) Where the Client is responsible for the network devices, modify access lists and firewall policies to permit scanning traffic to reach systems within scope of the SOW.

(h) Provide access to application and server ownership/operational risk manager with authority to approve patching.

(i) Responsible for selecting and maintaining any compliance regimes they wish to employ (NERC CIP, PCI DSS, NIST, etc.), and to inform NTT of their intentions, it is the Clients responsibility to determine if the actions taken by NTT comply with its compliance obligations.

(j) Remediate vulnerabilities for systems that the Client manages (NTT will remediate vulnerabilities on systems that they are responsible for managing)

(k) Provide connecting to Client PAM tooling

3 Service Specific Operations

NTT offers three Service Tiers for VMaaS. The service Tier must be selected as In Scope in the SOW, otherwise all are out of scope.
Tasks legend:

(a) Tasks marked as ✅ are included in the service for the specified Service Tier.

(b) Tasks marked as ❌ are not included in the service for the specified Service Tier.

Task	Description	Phase	Silver	Gold	Platinum
Perform monthly **Internal** scan	Perform monthly credentialed internal vulnerability scan on internal IPs for assets listed in SOW for vulnerability scanning service.	**Discover**	✅	✅	✅
Perform monthly **External** scan	Perform monthly external network-based vulnerability scan on Internet accessible IPs for		✅	✅	✅

	assets listed in SOW for vulnerability scanning service.				
Vulnerability scanning reports	Generate monthly Vulnerability scan report.	**Assess**	✓	✓	✓
Client Notification	Notify Client of vulnerabilities associated with unsupported or end of life systems.		✓	✓	✓
Portal	Generated reports available in the NTT Services Portal		✓	✓	✓
Vulnerability management and remediation reports	Generate monthly standardized Vulnerability management and remediation report.	**Prioritize**	✗	✓	✓
Information Security Manager (ISM)	Client receives support from an Information Security Manager who works to improve the overall security posture of the Client. See *Information Security Manager* section below in this description.		✗	✓	✓
Monthly review	ISM reviews findings and recommendations with Client in a scheduled monthly meeting. All calls are held remotely and are scheduled during the normal business work hours of the ISM.		✗	✓	✓
Awareness and classification of Client systems	Understand the Client's business critical applications, tag them, and categorize assets into relevant groups.		✗	✓	✓
Prioritize vulnerabilities and remediation efforts	Help the Client to prioritize vulnerabilities and focus efforts on remediation based on organizational risk		✗	✓	✓
Maintain audit trail of non-remediated vulnerabilities	Maintain an audit trail of Client decisions regarding non-remediated vulnerabilities.	**Remediate**	✗	✗	✓
Communications to asset owners	Provide communications to application and asset owner and/or operational risk manager to coordinate vulnerability risk mitigation and remediation.		✗	✗	✓
Remediation guidance	Provide remediation assistance for "Critical" and "High" rated operating system or managed application vulnerabilities for NTT hosted or managed systems. "Critical" and "High" are defined per the Common Vulnerabilities and Exposures ("CVE") standard. • For systems managed by the Client or other 3rd parties NTT will provide the scanning vendors published remediation advice to the asset owners. • For systems managed by NTT on behalf of the Client, the relevant NTT team will perform remediation actions in accordance with the scanning vendors published remediation advice. The ISM will log tickets and work with the teams responsible for remediation through to completion.		✗	✗	✓

Validation of successful remediation actions	Perform a post remediation scan to confirm that remediation actions have been successful, and the vulnerability closed.	**Validate**	✗	✗	✓
Remediation execution reporting	Information in the Vulnerability management and remediation report confirming validity of remediation actions. Confirmation will be provided in the standard monthly reporting cycle.		✗	✗	✓

4 Information Security Management

Information Security Management (ISM) is a component of NTT's VMaaS delivered by a designated member of the ISM team. The key functions of ISM include:

(a) Interpret and present the monthly Vulnerability management and remediation reports to the Client.

(b) Present findings and recommendations to the Client in a scheduled monthly meeting.

(c) Present recommendations on prioritizing remediation actions based on the severity of the vulnerability and criticality of the Client system. Where NTT manages the Client system, the ISM will coordinate the recommended remediation actions

4.2 Coverage

The availability of Information Security Management (ISM) is subject to applicable locations and shall be the local time zone the Registered Office location of the SOW Signatory of the Client, unless otherwise specified in the SOW.

4.3 ISM Tasks Included in the Silver Service Level

ISM Support not provided in the Silver Service Level.

4.4 ISM Tasks Included in the Gold Service Level

Task	Description	Frequency	Limitations/Out of Scope
Monthly review	ISM reviews findings and recommendations with Client in a scheduled monthly meeting.	Monthly	All calls are held remotely and are scheduled during the normal business work hours of the ISM
Awareness and classification of Client systems	Understand the Client's business critical applications, tag them, and categorize assets into relevant groups.	Monthly	
Prioritize vulnerabilities and remediation efforts	Help the Client to prioritize vulnerabilities and focus efforts on remediation based on organizational risk	Monthly	

4.5 ISM Tasks Included in the Platinum Service Level

All of the above tasks included in *Gold,* plus the following:

Task	Description	Frequency	Limitations/Out of Scope
Maintain audit trail of non-remediated vulnerabilities	Maintain an audit trail of Client decisions regarding non-remediated vulnerabilities.	Monthly	
Communications to asset owners	Provide communications to application and asset owner and/or operational risk manager to coordinate vulnerability risk **mitigation** and **remediation**.	Monthly	
Remediation guidance	Provide remediation assistance for "Critical" and "High" rated operating system or managed application vulnerabilities for NTT hosted or managed systems. "Critical" and "High" are defined per the	As needed	

	Common Vulnerabilities and Exposures (“CVE”) standard. · For systems managed by the Client or other 3rd parties NTT will provide the scanning vendors published remediation advice to the asset owners. · For systems managed by NTT on behalf of the Client, the relevant NTT team will perform remediation actions in accordance with the scanning vendors published remediation advice. The ISM will log tickets and work with the teams responsible for remediation through to completion.		
Validation of successful remediation actions	Perform a post remediation scan to confirm that remediation actions have been successful, and the vulnerability closed.	As needed	
Remediation execution reporting	Information in the security operations report confirming validity of remediation actions. Confirmation will be provided in the standard monthly reporting cycle.	As needed	

5 Technology Configurations

Technology Configuration may include scanning software deployed in the Client environment (Internal scanner), scanning software located on the Internet (External scanner), and software installed on Client systems (Agents and Gateways).

Internal Scanners	
Description	Scanning software provided by the scanning vendor is installed on a system in the Client environment. The scanning software is used for scanning networks and systems that are not Internet facing and so can’t be reached by a scan from outside the Client environment. The scanning software is downloaded from the cloud providers authorized “Marketplace” store, and it is enabled with an activation key. The scanning software receives instructions from, and reports back to, the scanning vendor management console which is located on the Internet. Neither the Client nor NTT have access to the scanning software and should not attempt to gain access to it.
Setup Activities	NTT will provide the Client with details of the authorized scanning software that the Client needs to download from the cloud providers marketplace. NTT will provide an activation key that the Client can use to enable the software. NTT will provide details of the firewall and access list changes that the Client needs to make to allows the internal scanner to operate.
Client Responsibilities	The Client shall be responsible for downloading authorized copies of the software from the marketplace of their chosen cloud services provider, and for installing it on their internal network. The Client shall be responsible for the continued operation of the scanner through the supply of resources such as processing power, memory, disk space. The Client shall configure firewall rules and access lists to enable the scanner to reach areas of the internal network, and to contact the scanning vendor management system on the Internet. The client shall provide service account(s) for unmanaged servers/devices for the purpose of authenticated scans if applicable
NTT Responsibilities	NTT will provide the client with details of the authorized scanning software that the client needs to download from the cloud providers marketplace. NTT will provide an activation key that the client can use to enable the software. NTT will provide details of the firewall and access list changes that the client needs to make to allows the internal scanner to operate.
External Scanners	

Description	External scanning software is deployed at the scanning vendors locations on the Internet. It is used to scan a Client's external (Internet facing) systems. There is no software to install in the Client environment for external scanning
Setup Activities	NTT will provide details of the firewall and access list changes that the Client needs to make to allows the external scanner to operate.
Client Responsibilities	The Client shall configure firewall rules and access lists to enable the external scanner to reach areas of the Client's external network. The client shall provide service account(s) for unmanaged servers/devices for the purpose of authenticated scans if applicable
NTT Responsibilities	NTT will provide details of the firewall and access list changes that the client needs to make to allows the external scanner to operate.
Scanning Agents	
Description	Agent software can be installed on Client systems, and it will report information which is not possible to obtain using internal or external scans alone. NTT shall provide the Client with temporary access to an online repository so that they can download the agent software. The Client is then responsible for deploying the agent to their systems. NTT highly recommends that the Client incorporates the agent installation into their standard build process. After the initial download of the agent software NTT shall remove access to online repository. The scanning agent software receives instructions from, and reports back to, the scanning vendor management console which is located on the Internet. Neither the Client nor NTT have access to the scanning agent and should not attempt to gain access to it.
Setup Activities	NTT shall provide the Client with access to a secure repository for the initial download of the agent software. NTT shall provide instructions on how to configure the agent software. NTT will provide details of the firewall and access list changes that the Client needs to make to allows the agent software to send information to the scanning vendor management system on the Internet.
Client Responsibilities	The Client shall perform an initial download the agent software from the repository provided by NTT. The Client shall Install the agent software on their systems. The Client shall configure firewall rules and access lists to enable the agents to contact the scanning vendor management system on the Internet. The client shall provide service account(s) for unmanaged servers/devices for the purpose of authenticated scans if applicable
NTT Responsibilities	NTT shall provide the client with access to a secure repository for the initial download of the agent software. NTT shall provide instructions on how to configure the agent software. NTT will provide details of the firewall and access list changes that the client needs to make to allows the agent software to send information to the scanning vendor management system on the Internet.
Scanning vendor proxy (Gateway server)	
Description	In situations where the agent software cannot contact the scanning vendor directly, a proxy (gateway server) may be configured on the perimeter of the Client network. The gateway will receive information from the agent installed on the Client systems and pass it on to the scanning vendors management console on the Internet.
Setup Activities	NTT shall provide the Client with access to a secure repository for the initial download of the gateway server software. NTT shall provide instructions on how to configure the gateway server software. NTT will provide details of the firewall and access list changes that the Client needs to make to allows the gateway server to pass information to the scanning vendor management system on the Internet.
Client Responsibilities	The Client shall perform an initial download the gateway server software from the repository provided by NTT. The Client shall Install the gateway server software on their systems and ensure it has resources such as processing power, memory, disk space.

	The Client shall configure firewall rules and access lists to enable the gateway server to receive information from agents and to pass it on to the scanning vendor management system on the Internet.
NTT Responsibilities	NTT shall provide the client with access to a secure repository for the initial download of the gateway server software. NTT shall provide instructions on how to configure the gateway server software. NTT will provide details of the firewall and access list changes that the client needs to make to allows the gateway server to pass information to the scanning vendor management system on the Internet.

6 Service Transition

6.1 Tasks included in the Standard Transition

As part of the Service, the following tasks are included within the setup fee:

(a) Assign ISM for the Client and assign to delivery team.

(b) Coordinate with Client to schedule the Project Kick Off Meeting. Items may include:

(c) Timing of monthly calls

(d) Non-standard reporting

(e) User credentials required for credentialled scanning of assets.

(f) Assist with the configuration and deployment of scanning software and agents.

(g) Assist with the configuration of access rules and firewall policies to permit the scanning traffic.

(h) Verify the Client is configured appropriately within each service-dependent system.

(i) Run a discovery scan and confirm scans ran as expected.

(j) Archive Project Artifacts (workbook templates / playbooks etc.)

(k) Handover to SOC and ISM on the pre-agreed Service Commencement date.

(l) Maintain system architecture and infrastructure of the vulnerability scanning platform.

(m) Where NTT is responsible for the network devices, modify access lists and firewall policies to permit scanning traffic to reach systems within scope of the SOW.

(n) Where NTT is responsible for a Client system then they will perform the necessary actions. Where the Client or 3rd party are responsible, NTT will work with them to perform the work.

6.2 Tasks not Included in the Standard Transition

The following tasks are not included in the standard transition:

(a) Configure access rules and firewall policies to permit the scanning traffic (Where NTT is not responsible for network devices)

(b) Installation of Internal scanner software (where NTT is not responsible for management of the device)

(c) Installation of agent software (where NTT is not responsible for management of the device)

(d) Installation of agent gateway server software (where NTT is not responsible for management of the device)

7 Limitations

(a) NTT shall pass on the scanning vendors remediation recommendations to the Client in good faith.

(b) NTT shall not test or confirm the efficacy of remediation recommendations in advance of passing on the information.

(c) NTT shall not be responsible for any system outages, loss or damages caused as a result of following the scanning vendors remediation recommendations.

(d) NTT does not guarantee that remediation recommendations will fix the vulnerability in its entirety.

(e) No console access or self-directed access is allowed by Client

(f) All use of the VMaaS service must be for Clients internal use only

(g) No attestation or certified statement will be provided by NTT

8 Out of Scope

(a) Direct access to NTT's vulnerability management platform is not provided.

(b) Support for printers, mobile devices, transient devices and/or VOIP phones is out of scope.

(c) Remediation of vulnerabilities associated with unsupported or end of life systems.

9 Supported Environments

Only available for:

(a) NTT managed Client on-premises data center

(b) NTT Managed Private and Public Cloud

10 Special Terms and Conditions

(a) Client shall not (i) modify, adapt, alter, translate or create derivative works of the VMaaS Services or Documentation; (ii) reverse engineer, reverse assemble, disassemble, decompile or otherwise attempt to decipher any code used in connection with the VMaaS Services and/or any aspect of NTT or the VMaaS technology; (iii) access and/or engage in any use of the VMaaS Services in a manner that abuses or materially disrupts the assets, networks, security systems, of any third party; (iv) rent, lease, loan, or use the WAS Services to a third party via timesharing or as a service bureau; (v) market, offer to sell, sell, and/or otherwise resell the VMaaS Services to any third party; (vi) use the VMaaS Services other than in accordance with the Documentation; (vii) use the VMaaS Services to scan an asset, system or otherwise for which Client does not have the right or consent to scan; or (viii) remove, alter or obscure any proprietary notices on the VMaaS Services or any documentation. If Client is unable or unwilling to abide by a usage limit, then Client shall be liable for the fees for such excess usage. The VMaaS uses open-source software in its operation and Client grants permission for to use open-source software. Client will indemnify, defend and hold harmless NTT and its WAS provider against any claim, demand, suit or proceeding made or brought (including any damages, attorney fees and costs) against NTT or it's VMaaS provider by a third party alleging or arising from Client's use of the VMaaS Services in breach of this paragraph or not in accordance with applicable law, and Client may not settle any claim, demand, suit or proceeding unless it unconditionally releases NTT and VMaaS provider of all liability.

(b) Client grants NTT and NTT VMaaS provider Client's consent to hosting, copying, transmitting and displaying Client Data as necessary for VMaaS to provide the VMaaS Services, including without limitation, the provision of the standard support and the use of worldwide affiliates to provide the VMaaS Services. Client grants to NTT and the VMaaS provider and its Affiliates a worldwide, perpetual, irrevocable, royalty-free license to use and incorporate into its services any suggestion, enhancement request, recommendation, correction or other feedback provided by Client or Users relating to the operation of VMaaS or the related services. NTT has no obligation to maintain the data after the subscription for the VMaaS service has ended. All VMaaS software and any related software must be uninstalled at the end of the subscription for service. Client agrees to abide by any End User terms and conditions required by the VMaaS provider for select levels of access to systems.