Enhanced Security Services - NTT Led Security Incident Response Service

1 Overview of Service

NTT Led Security Incident Response Service is a premium service offering that provides the Client with a team of Security Incident Responders that utilize security tools including the Client requirement of NTT's standard Endpoint Detection & Response (EDR) agent on NTT-managed systems. The Security Incident Response Team (SIRT) will respond to cyber security escalations and incidents, for example such as:

(a) Business Email Compromise

(b) Ransomware

(c) Compromised/ Stolen Credentials

(d) Active Adversary (Hands on Keyboard)

(e) Denial of Service (DoS)

(f) Insider Threat

(g) Exfiltration of Data

(h) System Compromise

1.2 Optional Service for an Additional Fee

(a) Phishing Email Triage

2 Client Responsibilities

(a) As a requirement for Security Incident Response Services, client must approve the installation of the NTT provided and required standard investigation agent, NTT's standard EDR (Endpoint Detection and Response) solution on all NTT-Managed systems. The agent license usage is billed per the pricing terms.

(b) For investigations into Client-managed systems, Client will be required to install the NTT's standard EDR (Endpoint Detection and Response) agents on the systems not managed by NTT that are part of the managed deployment scope.

(c) Investigations involving Client-managed systems will commence after deployment of the NTT standard EDR agent to ensure visibility into the Client environment and ability for the SIRT to effectively respond.

(d) Client is responsible for testing of Client systems and any impact to NTT SLAs, due to impact from Client or Client 3rd party security tools that are implemented as part of an incident or investigation.

(e) Client will coordinate tabletop exercises. If requested, NTT Security resources will participate in exercises.

(f) Client shall procure and coordinate any security forensics firm required by Client.

3 Service Specific Operations

Task	Description
NTT Security Incident Responder	For Clients with NTT Security Incident Response & Investigation as an In-Scope Service, the NTT Security Incident Responder shall be engaged, when security alerts show a probable or successful attack such as: • Business Email Compromise • Ransomware • Compromised/ Stolen Credentials • Active Adversary (Hands on Keyboard) • Denial of Service (DOS) • Insider Threat • Exfiltration of Data • System Compromise Optional Add-On Service- Phishing Email Triage
NTT Security Incident Response Coordination	The Security Incident Responder will coordinate with the Client and NTT resources to quarantine/contain the issue, maintain evidence if and as guided by a forensic firm, and guide the teams to assist in restoring the environment or systems to a pre-compromised state.
NTT Security Incident Response Activities	NTT security incident response activities may include the collection and analysis of volatile memory data, live acquisition, containment of current threat, updating of managed endpoint protection systems, and tracking and enforcement of Indicators of Compromise, updating Client on potential impact, and report writeup including Lessons Learned associated with high/critical severity cases.

Usage of Cyber Security Case Management Tool	NTT Security Incident Response Team will utilize an NTT-managed Security Orchestration Automation Response (SOAR) Cyber Security case management tool for incident response workflow management, security incident documentation and tracking. Direct Client access to SOAR tool is not available.
Standard Investigation Agent Deployment - Servers	Deploy and manage the NTT standard investigation agent to NTT managed servers.
Standard Investigation Agent Deployment - Endpoints	Deploy and manage the NTT standard investigation agent to in-scope NTT managed Client endpoints. Note: Clients endpoints are laptop or desktop machines but not mobile devices, such as phones or tablets.
Standard Investigation Agent Deployment - Mobile Device	Deploy and manage the NTT standard investigation agent to in-scope NTT managed Client phones or tablets.
Standard Investigation Agent Deployment - non-NTT Managed Servers	Client to deploy the NTT standard investigation agent to in-scope non-NTT managed servers.
Standard Investigation Agent Deployment - non-NTT Managed Endpoints	Client to deploy the NTT standard investigation agent to in-scope non-NTT managed Client endpoints. Note: Client endpoints are laptop or desktop machines but not mobile devices, such as phones or tablets.
Standard Investigation Agent Deployment - non-NTT Managed Mobile Device	Client to deploy the NTT standard investigation agent to in-scope NTT managed Client phones or tablets.
Deploy Additional Client 3rd party Agents	Deploy Client vendor provided security investigation software packages on NTT managed client systems from Client's authorized 3rd party forensic company when deemed necessary by Client.
Utilize Security Incident Response Plan	Use NTT's template Security Incident Response plan, or if agreed upon, a customized Security Incident Response plan for duration of an incident.
Monthly Recurring 30 Minute Security Review Summary	When requested, NTT will review current usage of Security Incident Response (SIR) cases, trends and issues.
Quarterly Recurring 1 Hour Security Leadership Review Summary	When requested, review current usage of SIR service, trends, and industry issues with security leadership member.
Root Cause Analysis	When technically able, NTT will determine threat actor root cause to be included in incident summary.
Preserve Evidence	Retain a copy of NTT gathered investigative security incident information for impacted system(s) for up to 14 business days from conclusion of the recovery of the affected system.
Security Investigation Data	Upon request and within the above retention period, NTT will provide gathered security investigation data to the Client or their 3rd party forensic company.
Dedicated Security Incident Report	Provide SIR report, based upon the NTT template, with a timeline of all of the Security Incident activities, actions, follow-ups and root causes (if root cause was determined) for high and critical severity cases.

4 Supported Environments

(a) NTT managed client on-premises data center

(b) NTT managed private and public cloud

5 Billing

Charges shall be based on a fixed fee for a block of hours per month for a Cybersecurity Case Life Cycle time open to close (CCLC Rate) per month counting all hours (the Baseline). The client will not receive credit for hours that not used in month, in the event that the client exceeds the block of hours by more than 20% (twenty percent) more than 3 (three) in a 6 (month) window, NTT will adjust the charges to be the hours of the average of the highest 3 (three) months multiplied by the CCLC Rate which shall become due in the month of the

adjustment is made, this new Baseline shall become the Baseline and shall continue for the remainder of the SOW.

6 Out of Scope

(a) Reverse engineering prohibited by the licensor or manufacturer, or other prohibited activities are out of scope.

(b) Preserving evidence in excess of the above time period is out of scope, but if requested by Client via change control and requested within the retention period above, captured data evidence can be retained for the duration Client's internal or 3rd party forensic company dictates. Additional storage and backup rates shall apply.

(c) Enhanced Security is not a standalone offer, and can only be included when standard security is in Scope in the SOW.