Digital Forensics Incident Response Compromise Assessment

1 Overview of the Service

This is a proactive service targeted toward customers who want a review of their network traffic entering and departing their networks and gateways as well as an assessment of endpoint systems for anomalies and threats which may exist.

1.1 Technologies for the DFIR Service

(a) The tools stated within this list may be used with NTT's sole discretion to perform the compromise assessment at no additional cost to the Client, the Client agrees to abide by any required End User License Agreement:

(i) MixMode Network Sensor – Network Packet Capture

(b) NTT may exchange this software and require the Client to execute a new End User License Agreement in its sole discretion.

2 Client Responsibilities

(a) **Point of contact:** The Client will appoint a primary point of contact for NTT personnel to liaise with throughout the engagement to gather environment-specific information (e.g. network diagrams, configuration details), schedule deployment activities, conduct ongoing updates and support the successful completion of DFIR activities. The primary method of communication will be email.

(b) **Approve Tool Deployment**: The Client must approve the installation of NTT's specific DFIR tool sets, as stated in the Technologies for the DFIR Service section. The agent license will not be charged to the Client as part of the investigation.

(c) **Agree to Tool Use:** Client must comply with the use of NTT's DFIR Supported Technologies to conduct the compromise assessment, which may be updated by NTT from time to time. Any tool deployment will not typically exceed 30 days unless stated otherwise.

(d) **Agree Data Residency:** The Client will agree upfront on the geolocation for forensic and evidentiary data that will be exfiltrated to conduct the DFIR engagement.

(e) **Data Storage:** Evidentiary/forensic data (e.g. log data, forensic images etc) that are collected from the Client as part of the engagement will be deleted 90 days from the conclusion of the DFIR engagement. The Client is required to provide advanced notification (no less than 30 days from the conclusion of the DFIR engagement) if the data collected is required beyond the 90-day limit. Any costs associated with the extended storage and or transport will be billed to the Client.

(f) **Remote Environment Access:** The Client will provide access, as required and in the format and method requested by NTT, to their network or other required assets for the purposes of the compromise assessment.

(g) **Provide Historical Data:** At the onset of the engagement, NTT will request specific data containers. All data that has been collected and stored for the last month should be provided by the Client. Below is a list of data that may be requested, this list is not all-inclusive:

(i) Firewall Logs

(ii) Security Logs

(iii) VPN Logs

(iv) Active Directory

(v) Admin Account information

(vi) Administration Account IDs

(vii) Names of employees who had/have access to each account

(viii) PCAPs

(ix) Netflow

3 Service Specific Operations

Task	Description
Tool Deployment	Identify, configure and deploy tools at internet egress points and on critical servers and endpoints within the environment for a 30-day period
Traffic Monitoring	DFIR consultants will monitor trajectory traffic into and out of each system within scope.
Log Analysis	Analyze an organization's logs to search for anomalous nefarious activity

Data Collection	Data will be gathered at the internet egress points to enable threat hunting.
Threat Hunting	Identify Indicators of Compromise (IOC), including malware artifacts or network traffic activity
Red Flag Identification	Identify and report on any red flags that are identified as part of the investigation.
Deep Dive Analysis	Deep dive log analysis if applicable, to investigate and attempt to establish facts related to a potential security breach
Report Generation	Provide a report detailing the actions taken, any red flags identified as part of the investigation, and remediation recommendations.

3.1 DFIR Retainer Hours

(a) This section is out of scope for Clients acquiring this service as a standalone offering or not in combination with DFIR.

(b) NTT enables Clients that have selected Gold and Platinum DFIR retainer packages to utilize unused retainer hours towards the deployment of this service. These Clients can utilize this service anytime within their contracted term (up to the last 60 days) and are strongly encouraged to do so.

(c) Gold Clients can use **no more than 50%** of their unused retainer hours towards additional IR-related services. The balance of unused hours must meet or exceed 60 hours to deploy this service.

(d) Platinum Clients **can use 100%** of their unused retainer hours towards this service. The balance of unused hours must meet or exceed 60 hours to deploy this service.

4 NTT DFIR Deliverables

The main deliverables for this service include:

Deliverable Summary	Deliverable
Red Flag Report	Summary of all the red flags identified as part of the investigation and a rating of the potential impact.
Prioritization & Recommendations	1x report (Microsoft (MSFT) Word / PowerPoint) detailing a prioritized view of the red flags and remediation recommendations for the top 5 red flags.

5 Billing

Standalone: Charges shall be based on a fixed fee for the work to be carried out. Any further investigation, remediation or forensic activities that may be required will be charged separately as agreed via a new statement of work.

Utilizing Gold or Platinum Retainer Hours: A Client can utilize their unused retainer hours as a means of payment for the service. A total of 60 hours will be deducted from the Clients remaining DFIR retainer hours.

6 Limitations

(a) The compromise assessment will be carried out via remote means only and no onsite delivery will occur.

(b) The compromise assessment will not go beyond the identification and prioritization of identified threats within a Client's environment. Any further remediation activities are subject to a new SOW.

(c) The compromise assessment tool deployment will last no longer than a 30-day period.

7 Service Transition

Transition Task Summary	Overview
NTT Kick-off to introduce the service and confirm details	1x two-hour remote workshop ((Video Teleconference (VTC), e.g., Microsoft Teams)) and kick-off deck (MSFT Word / PowerPoint) providing details of the assessment.
NTT & Client agree on target systems that will form part of the assessment	List of systems that will be targeted as part of the assessment agreed by the Client and NTT.
NTT & Client to agree and deploy any data capture tools as needed.	1x two-hour remote meeting to agree tool deployment. NTT DFIR tools deployed on the Client environment as required.

8 Service Transition Out of Scope

Any actions not specified within the service transition scope.

9 Out of Scope

(a) Any activity not specified as in scope.

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

(c) Preserving findings in excess of 90 days is out of scope, but if requested by the Client findings can be retained for the duration the Client's internal or 3rd party forensic company dictates. Additional storage and backup rates shall apply.

(d) Any remediation or forensic activities that are required in order to neutralize the identified red flag(s).

10 Service Specific Terms and Conditions

The following terms and conditions apply to this Service Description and any dependent thereon, and specifically supersede any conflicting terms and conditions in any other agreement between the parties.

- Client warrants that it has obtained all consents necessary for the data to be collected and used on its behalf for compromise assessment and that it has a legal basis for requesting such information (excluding consents from NTT employees and agents) and shall indemnify, defend and hold harmless NTT for the use of this information for this Service.
- Client expressly agrees to enable the deployment of NTT DFIR tooling within the Clients environment if required
- All data related to the investigation will be deleted 90 days after the conclusion of the investigation, unless expressly requested otherwise. All costs associated with storing data beyond this time will be billed to the Client.
- NTT shall own all rights, title and interest to any Work Product, Intellectual Property, code or otherwise, developed as part of this Service. In the event Client provides any ideas, suggestions, improvement, Work Product, Intellectual Property, code or otherwise as a suggestion, improvement or otherwise required to enable this Service, Client hereby assigns all rights, title and interest to NTT. Client expressly agrees to the use of Third Party and Open Sources components and services in this Service and agrees to abide by all required terms and conditions of any third-party product.
- No Control Rule compliance will be included in this Service. This Service Description and Service may be cancelled at any time, in NTT sole and absolute discretion. NTT reserves the right to replace, change, alter, or not provide any third-party software required to perform the Services and any Service that depends on those items may be terminated by NTT.
- An investigation will be conducted, which may include deployment of analytical tools or transfer of forensic images to regional forensic processing servers (in line with local data processing regulations/compliance requirements).
- NTT will use a blend of on-shore and off-shore resources to securely deliver the service unless directly requested or legally complied not to. Any additional costs associated with 100% on-shore or a change in the delivery will be charged to the Client accordingly.