Digital Forensics Incident Response Runbook Development

1 Overview of the Service

Each Runbook is designed on a case-by-case basis and is designed to align against specific threats to the business i.e. Ransomware, Phishing, DDoS, etc.

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, process & tool specific information (e.g. network diagrams, configuration details), Schedule and conduct workshops, updates and support the successful completion of runbook development. The primary form of communication will be written (Email).

(b) **Agree Runbook Scope:** The client will be required to agree the scope of the runbook before development, which shall not exceed 10 hours per run book.

3 Service Specific Operations

Task	Description
Remote Scoping	Remote session to understand and further explore the client's requirements for developing the incident response runbooks. Documenting and agreeing on the specific runbooks(s) that will be developed.
Run Book Development	Develop each Runbook(s) against a defined threat source (in agreement with the client) and utilizes all of the technology and tools available to the local security team.

3.1 DFIR Retainer Hours

(a) *This section is out of scope for clients acquiring this service as a standalone offering.*

(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 10 hours (per run book) 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 10 hours (per run book) to deploy this service.

4 NTT DFIR Deliverables

The main deliverables for this service include:

Deliverable Summary	Deliverable
Runbook	A completed runbook(s), number of runbooks to be confirmed in the SOW.

5 Billing

Standalone: Charges shall be based on a fixed fee for the work to be carried out, which shall not exceed 10 hour per runbook, otherwise any additional work shall be billed at NTT's current DFIR list rate. 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 10 hours will be deducted from the client's remaining DFIR retainer hours per runbook.

6 Limitations

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

(b) The runbook development engagement will provide guidance and no DFIR tools or ongoing support will be provided beyond the engagement conclusion.

(c) A high-level tactical process flow (incident runbook) will be defined in Microsoft Word / PDF based on the Client's security controls (excluding configuration of specific security technology) however, no automation scripts will be created as part of the engagement.

(d) An engagement will include the development of a single runbook unless otherwise agreed and stated on the statement of work.

7 Service Transition

Transition Activity	Overview
Kick-off to introduce the service and confirm details	1x Remote meeting (Video Teleconference (VTC), e.g., Microsoft Teams) and kick-off deck (MSFT Word / PowerPoint) providing details of the engagement and confirmation of the scope.

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) The provision of any tooling to support DFIR activities beyond the conclusion of the engagement.

(c) On-going DFIR support or training beyond the conclusion of the engagement.

(d) The development of more than a single runbook unless stated otherwise on the statement of work.

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.