Digital Forensics Incident Response Incident Response Plan Testing (Tabletop Exercise)

1 Overview of the Service

As more organizations fall victim to cyber-attacks, they are now measured by how well they respond to such attacks.

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 the tabletop exercise, conduct ongoing updates, and support the successful completion of the exercise. The primary form of communication will be written (Email).

(b) **Agree Scenario:** The client is responsible for agreeing to the testing scenario that will be deployed before the exercise can be conducted.

(c) **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 IR plan testing.

(d) **On-Site Environment Access:** For on-premise activities, the client will provide access to the systems in scope, workspace, internet access, and other necessary resources required to successfully conduct the exercise.

3 Service Specific Operations

Task	Description
Kick Off	A session to confirm the service approach, identify key resources, incident response-related material, and any additional requirements for a successful engagement.
Documentation Review	A review of the Client's existing incident response plans and artifacts provided to NTT during or before the kick-off meeting.
Test Scenario Development	Define and agree on the test scenario that will be deployed within the exercise. The scenario will be based on the Client's industry vertical, threat landscape, and any specific client requirements.
Scenario Deployment & Assessment	Host tabletop sessions with the Client’s security team (and wider participants). Assessed on ability to follow IR Plan and where there are gaps in capability.
Incident Response Observations	During the scenario deployment, NTT DFIR consultants will document their observations of the response activities.

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 40 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 40 hours to deploy this service.

4 NTT DFIR Deliverables

The main deliverables for this service include:

Deliverable Summary	Deliverable
List of scenario observations	1x list of observations in Microsoft (MSFT) Word or PowerPoint.
Prioritisation & Recommendations	Report (MSFT Word / PowerPoint) detailing strengths and weaknesses in responding to the tabletop scenario. A prioritised list of recommendations to improve the client's response maturity.

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. Any work beyond 40 hours shall be billed at NTT's current list rate for DFIR.

Utilising Gold or Platinum Retainer Hours: A client can utilize their unused retainer hours as a means of payment for the service. A total of 40 hours will be deducted from the client's remaining DFIR retainer hours.

NTT may perform the assessment remotely, from Security offices, or onsite at Client facilities, unless travel is not allowed by the government (global pandemic, etc). In the event on-site support is requested, the Client agrees to reimburse NTT Security for all travel and expenses with a minimum day of eight (8) hours while traveling.

6 Limitations

(a) The IR Plan Testing includes the development and deployment of a single scenario to be agreed upon by the client and NTT. Any further scenario development or deployment will require a separate SOW.

(b) The NTT consultants will provide guidance and support where appropriate but will not be directly responsible for any remediation activities during the test scenario.

(c) No NTT tooling will be deployed to support the response capabilities of the organization during the test scenario.

7 Service Transition

Transition Summary	Overview
Kick-off to introduce the service, confirm details and review existing documentation	1x Remote or onsite workshop (Video Teleconference (VTC), e.g., Microsoft Teams)) and kick-off deck (MSFT Word / PowerPoint) providing details of the assessment.
Tabletop Scenario Creation	1x tabletop scenario that will be run as part of the exercise

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 development or deployment of more than a single table top scenario.

(c) Re-running the same scenario more than one time if not directly expressed on the SOW.

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