Digital Forensics Incident Response – Incident Response (IR) Plan Design

1 Overview of the Service

NTT DFIR consultants will work with clients to review and evaluate policies against industry best practices, regulatory and compliance requirements, and develop an appropriate Incident Response Plan tailored to the organization's specific needs.

2 Client Responsibilities

Point of contact: The client will appoint a primary point of contact for NTT personnel to liaise with throughout the engagement to gather specific information (e.g. existing incident response plans and other IR-related material), schedule and attend workshops, and support the successful completion of IR Plan Design. The primary method of communication will be email.

3 Service Specific Operations

Task	Description
Baseline	Conduct a rapid baseline of the existing client IR procedures and processes.
IR Requirements	Define and capture the list of client incident response plan requirements this may include: compliance & regulatory requirements, threat landscape, resource constraints etc.
IR Plan Workshop(s)	Conduct IR Plan workshops as required to develop the security operations incident response plan (excluding legal, compliance, client communications and any other response outside of security operations) with the client's security team.
IR Plan	Define a bespoke Plan aligned to the client's requirements which includes elements such as Workflows, Communications Plans, Roles and Responsibilities etc.

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 utilise 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
IR Plan Plan	1x incident response plan in Microsoft (MSFT) Word / PowerPoint document.

5 Billing

(a) Standalone: Charges shall be based on a fixed fee for the work to be carried out, any additional hours beyond 40 hours shall be out of scope and subject to NTT's current list rate for DFIR. Any further investigation, remediation or forensic activities that may be required will be charged separately as agreed via a new statement of work.

(b) 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 40 hours will be deducted from the client's remaining DFIR retainer hours, as limited above.

6 Limitations

(a) The IR Plan Design will be carried out via remote means only and no onsite delivery will occur.

(b) The IR Plan Design will last no longer than 40 billable Hours.

7 Service Transition

Deliverable Summary	Deliverable
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 IR plan design process.
Baseline & Requirements Gathering Workshop	1x eight-hour workshop to discuss the existing IR response processes and procedures, and define a list of incident response plan requirements.

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 deployment of any DFIR tooling to enable the incident response plan.

(c) Any ongoing development of the incident response plan beyond the conclusion of the engagement.

(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.