Digital Forensic Incident Response (DFIR) OT Retainer Services

1 Overview of the Service

The NTT Digital Forensic Incident Response (DFIR) OT Retainer services assist an organization to effectively prepare, respond, contain, and rapidly remediate from a wide array of cyber incidents involving their IoT/OT environments.

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

(a) Magnet Axiom - Digital Investigation, Forensics & Reporting

(b) MixMode Network Sensor – Network Packet Capture

(c) Forensic Toolsets (FTK, EnCase, X-Ways, Axiom Cyber)

(d) Intella – Email Investigation & eDiscovery

(e) Cellebrite – Mobile Device Forensics

(f) Claroty – OT Visibility & Threat Detection

(g) Nozomi – OT Visibility, Detection & Analysis

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**: As a requirement for DFIR service, a client must approve the installation of NTT's specific DFIR tool sets, as stated in the Overview of the Service. The agent license will not be charged to the client as part of the investigation.

(c) **Agree to Tool Use:** The Client must comply with the use of NTT's DFIR Supported Technologies to conduct the DFIR engagement, which may be updated by NTT from time to time.

(d) **Agree Data Residency:** The customer will agree and approve 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 Digital Forensics and Incident Response (DFIR).

(g) **Data Preservation:** In the event of an applicable cyber security incident, the client will use its best efforts to preserve forensic findings to support the DFIR engagement.

(h) **Unused Retainer Hours:** The client is responsible utilising their unused retained hours for additional IR-related services (if required) within the contract anniversary. These additional IR-related services must be agreed with NTT no later than 60 days before the contract anniversary. NTT will conduct quarterly meetings to support the client in activating these services

3 Service Specific Operations

NTT offers one service level for DFIR OT Retainer with 120 total hours available.

Feature	Description
Retained Hours	The number of retained hours that can be utilised for DFIR-related activities per year before additional hours are required.
Remote Incident Response[1]	Remote incident response 24x7x365 within SLO to initiate phone contact with the client from a DFIR consultant.
Forensic Data Storage	Forensic data, by default, will be stored for up to 90 days
Tool Deployment	Deploy and manage NTT investigation / forensic tools on endpoints, servers, network and OT technologies (if required) when an incident occurs.

Quarterly Check-ups[2]	Quarterly checkups to establish if there have been major incidents or new technologies which are important to know prior to a DFIR engagement

1 Remote response SLO is 4 hours.

2 Any time associated with the quarterly meetings will be deducted from the Client's total retainer hour pool.

3 Any travel time will be charged at a minimum of 8 hours.

Task	Description
Incident Response Plan	Utilise NTT's standard incident response plan or if agreed upon, a client provided Security Incident Response plan for the duration of an incident
Onboarding & IR Plan Assessment	Remote onboarding session to understand the Client's network, estate and to agree on the IR processes & practices
Incident Response Identification	Collate log info on servers/endpoints or network technologies. Conduct rapid root cause analysis, and identify incident damage and residual risk. Maintain findings in line with client requirements.
Incident Containment	This may include the collection and analysis of volatile memory data, live acquisition, updating of managed endpoint protection systems, endpoint/server isolation, and tracking and enforcement of Indicators of Compromise.
Incident Eradication	Provide the client suggestions on how to handle and execute the eradication process.
Digital Forensics	Analysis to include forensic image (Windows / Linux), memory forensics, malware analysis, network forensics or log file analysis as and when required.
Reporting	Provide final DFIR report including timeline and analysis findings and recommendations

Actions	Outputs
Upon initial call from the client, NTT to discuss the symptoms to understand the scope, current, and residual risk from the incident.	Remote meeting (Video Teleconference (VTC), e.g., Microsoft Teams) and document the incident as stated within the call.
NTT to provide an Incident Action Plan.	Action plan detailing all known incident details and governance/escalation points and high-level next steps.
The Client to accept the deployment of any DFIR tools as needed.	Accept DFIR tool deployment. NTT DFIR tools are to be deployed on the Client's environment as required.
NTT to discuss initial findings collection and delivery.	Remote VTC session and documented summary of findings collection.
NTT to define, agree and implement a strategy to limit the damage by containing the incident via appropriate procedures.	Documented high-level containment strategy and VTC to discuss if required. Deployment of tools, techniques, and procedures in line with the agreed strategy to contain the incident.
NTT to help eradicate the attack of the incident and its counter effects by providing guidance and instructions to on-site client security staff.	Remote VTC session(s)
NTT to triage and/or provide deep dive analysis to understand the what, when, where, who, why, and how.	Microsoft (MSFT) Word / PowerPoint document and/or remote VTC
NTT to identify the root cause, recognize the intrusion method, and determine the attack vector where possible based on findings.	MSFT Word / PowerPoint document and/or remote VTC
NTT to support and assist client security staff for business recovery.	Remote VTC session(s)

NTT to provide status updates (cadence to be agreed with the client during the agreement of the incident action plan).	MSFT Word / PowerPoint document that tracks the incident and provides ongoing updates.
NTT to conduct the following based on the scope of the incident and the goals of the client: · Acquire forensic images and provide forensic analysis · Provide advanced network, malware, IOC analysis · Provide advanced log analysis	Document results from forensic analysis, network, malware, IOC analysis, and log analysis in MSFT Word or MSFT PowerPoint as required.

4 Additional IR Related Services

NTT provides a number of additional IR-related services which can be deployed alongside the retained hours to improve an organisation's ability and capacity to respond to an incident. For further information on the additional IR-related services please see the service descriptions.

Unused Hour Utilisation: Clients utilising this service can deploy additional IR-related services anytime within their contracted term (up to the last 60 days) and are strongly encouraged to do so. Clients can **either use** their unused retainer hours or acquire these services for a fee.

Clients can use **no more than 50%** of their unused retainer hours towards additional IR-related services. The unused hours must meet the minimum number of hours to complete an additional IR-related service (e.g. DFIR Knowledge Transfer requires 40 hours) otherwise a fee will be charged for the outstanding hours.

5 NTT DFIR Deliverables

The main deliverables include the following:

Deliverable Summary	Deliverable
Deliver a Digital Forensic Incident Response Report	Document report in MSFT Word / PowerPoint. The report will include; · Executive Summary · Consultants assigned to the investigation · Timeline analysis · Detailed findings on all findings analyzed · Recommendations as identified

6 Billing

(a) Charges shall be based on a fixed fee upfront for a block of hours per year, to be used within the contract year. The client will not receive credit for hours that not used within the year and all hours will expire at the end of the contract year upon which they are granted.

(b) If total hours identified within this SOW are not sufficient to complete the Digital Forensics Incident Response Retainer Services requested by the Client, the Client agrees to work in good faith with NTT to either:

(i) Amend this SOW to include additional hours and/or fees.

(ii) Conclude Digital Forensics Incident Response Retainer services.

(c) Upon utilization of the initial annual hours, the Client will be charged at the additional hourly rate provided in the SOW until the Client directs NTT to stop work.

(d) If the client requires Additional IR Related Services and this cannot be covered by the remaining retained hours, the client will be billed accordingly.

(e) NTT may perform Digital Forensics Incident Response Services remotely or from NTT offices. In the event on-site support is necessary, the Client agrees to reimburse NTT for all travel and expenses with a minimum day of eight (8) hours while traveling.

(f) Any and all onsite delivery will be incurred at an increased hourly consumption rate of 1.5.

(g) Travel related to the execution of the DFIR OT Retainer will be billed at a minimum of 8 hours per travel day.

(h) An industrial control system (ICS) consultant may be required for certain clients to conduct a baseline of the OT infrastructure. This will be determined, documented and priced in the statement of work if applicable.

(i) In certain instances dedicated hardware will be required for the deployment of NTT tooling (Clarorty & Nozomi), if this is the case it will determined, documented and priced in the statement of work.

7 Limitations

(a) The retained hours within the scope expire at the contractual anniversary. Any additional hours during a DFIR incident declared by the Client shall be billed at NTT's current rate or rate card provided in the SOW and updated as allowed by the Agreement.

(b) Digital Forensics Incident Response services may include forensic analysis. Certain countries, states, counties, cities, or other jurisdictions ("Governmental Authority") may not allow the admission or other use of the findings resulting from any such forensic analysis in any legal proceedings unless the person or entity conducting the forensic analysis is properly certified, licensed, registered or otherwise expressly approved to engage in or conduct forensic analysis and related activities. NTT does not warrant, represent, or covenant, and expressly disclaims any warranty, representation or covenant, that it is certified, licensed, registered or otherwise approved by any Governmental Authority to engage in or conduct forensic analysis or related activities, or that any findings provided by NTT based on its forensic analysis will be admissible in any legal proceedings.

(c) For clients falling under GDPR jurisdiction, NTT does not take responsibility for breach notification or other notifications or communications required by the client within GDPR.

(d) NTT will not assist with data types/data classification of data impacted by incidents or creating/drafting crisis communication.

(e) Any licensing for specific tooling deployed during an investigation will not be carried over beyond the duration of the investigation.

8 Service Transition

Pre-service activation remote workshop:	
Kick-off to introduce the retainer package and confirm details	1x two-hour remote workshop (VTC). Provide an overview of the package applicable to the client, timelines, points of contact and features that are available.
Provide process and details on how to engage DFIR Team	Included as part of the kick-off workshop. Provide client-defined documents on the contract process and procedures.
Conduct discovery of assets, environment, incident response process, and people	Workshop to define list of discovery findings in MSFT Word / PowerPoint.
Review the Clients Incident Response Plan, if available	1x two-hour remote workshop (VTC) to discuss and confirm understanding of the response plan.

9 Service Transition Out of Scope

Any actions not specified within the service transition scope.

10 Out of Scope

(a) Any activity not specified as in scope.

(b) Continuous management of Client incidents including coordination of third parties beyond the statement of work.

(c) Any customer notification(s) or notification to government / regulatory agencies as legally mandated.

(d) Any communications or negotiations with threat actors during Ransomware attacks.

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

(f) 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.

(g) Any travel to client premise(s). Onsite support is out of scope unless expressly agreed upon within the statement of work.

11 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 DFIR service 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.
- If Client exceeds the retained hours in scope in the SOW, NTT reserves the right to stop any further engagement until the client acquires an additional hours. NTT shall make commercially reasonable efforts to notify the Client when they near the total utilization of the retained hours.
- Client expressly agrees to:
  - Use the Services only in accordance with this Service Description, the Documentation, the SOW, Contract, and the Agreement;
  - Enable the deployment of NTT DFIR tooling within the clients environment if required

- In the event the Client completes the required documentation to enable disabling of systems to allow NTT to respond to select discoveries made through the Service, Client expressly allows NTT to disable, shutdown or otherwise stop the functionality of any device in scope for this Service and Client waives all claims for any and all damages related to that activity and must execute a response action waiver before any action will be taken.
- All data related to the investigation and response activities 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. NTT in its sole and absolute discretion may allow Client access to select code upon Client's agreement to NTT's Code License.
- 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 as per the plan (dependent upon the engagement type), 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 delivery will be charged to the client accordingly.
- All SLO are objectives only and shall no penalties or service credits shall be paid.