

Managed Detection and Response

1 Overview of the Service

NTT's Managed Detection and Response (MDR) is a turnkey service focused on quickly detecting and effectively responding to cybersecurity threats, using advanced analytics, threat intelligence, expert-driven threat hunting and validation capabilities.

NTT will deploy Required Operational Technologies and Optional Operational Technologies as required and necessary used exclusively for the delivery of the MDR Service in the Client's Azure environment within the specific limits as specified in the SOW Service Offering table, except as required in the Client Responsibilities section.

2 Requirements

2.1 Required Operational Technologies for the MDR platform

- (a) Azure Sentinel
- (b) Azure Log Analytics Workspace (LAW)
- (c) Azure Logic Apps (Security Orchestration, Automation and Response platform)

2.2 Optional Operational Technologies for the MDR platform

- (a) Azure Blob Storage
- (b) Azure Data Explorer
- (c) Azure Log Analytics Workspace Data Archive
- (d) Azure VPN Gateway
- (e) Azure Syslog Forwarder that is located in Client Azure Tenant, must be in a load balanced active-active pair to ensure high availability.
- (f) Azure Load Balancer. An Azure Load Balancer is required for all Azure Syslog Forwarders.

2.3 Access Management Requirements

In order for NTT to manage the Client's environment, the following requirements must be met:

- (a) Azure Subscription (provided by CSP, Direct or EA) with Owner/Contributor role. In case of Client EA Enrollment, the Governance Hierarchy must be defined and provided by the Client; the Services Administrator role must be provided to NTT.
- (b) As NTT uses Azure Lighthouse to deliver the service, Client must delegate all resources under management to NTT with a Contributor role.
- (c) Allow Application registration in Azure Active Directory for monitoring and consumption tooling.

3 Client Responsibilities


- (a) Client will configure all in scope devices in accordance with the requirements of the Service and NTT instructions, unless specified otherwise in the SOW.
- (b) Client will ensure that all logs from in scope devices, not managed by NTT, are sent to the MDR service platform.
- (c) Client will provide connectivity API keys to log source and device connection.
- (d) Client will install and configure any additional Syslog Forwarders required within their estate. "Additional" to be defined as On-Prem, Client systems or other public cloud for example AWS, specifically excluding Azure, unless otherwise specified in the SOW.
- (e) Client will provide access, as required, to their network or other required assets for the purposes of Digital Forensics and Incident Response (DFIR).
- (f) Client will determine data retention period for each Log Analytics Workspace.
- (g) Client will delegate authority to NTT engineers to contact the technology vendor or any other Client vendor directly and provide any required licenses, use rights and access to NTT.
- (h) Client will provide all authorization, use, rights, licenses or as otherwise required by NTT.
- (i) Client will maintain an active Azure subscription that is available and supported by Microsoft and provide all access, rights, use, and licenses as required by NTT to provide this Service.
- (j) Client must comply with NTT's MDR Supported Technologies list for ingest, which may be updated by NTT from time to time.
- (k) Client must complete a Response Action Agreement before NTT will perform a Response Action. In the event, no Response Action Agreement is completed by the Client and accepted by NTT, no Response Action will be taken by NTT.


- (l) Client will be responsible for maintaining an authorized list of users and/or a distribution list for notification of MDR Incidents detected by the MDR service. Client will be deemed to have accepted notification of an incident upon NTT's notification to the agreed recipients.
- (m) Upon notification of an MDR Incident by the MDR service, the Client is responsible for activities associated with triage, investigation and security incident management in accordance with the recommendations provided by NTT in the MDR Incident Report.
- (n) Where NTT is responsible for operational management of a CI which requires remediation as part of the security incident or MDR incident response, Client is responsible for coordinating overall incident response, including raising appropriate incidents and/or Service Requests with NTT, unless mutually agreed in a SOW for support to be provided for the CI.
- (o) Client will log Requests for NTT to provide DFIR service support where the Client would like NTT to provide DFIR services related to a Client Security Incident. Refer to DFIR service scope as defined within section 3 (Service Specific Operations).



















4 Service Specific Operations

NTT offers three Service Tiers for MDR. The service Tier must be selected as In Scope in the SOW, otherwise all are out of scope.

Tasks legend:

(a) Tasks marked as  are included in the service for the specified Service Tier.

(b) Tasks marked as  are not included in the service for the specified Service Tier.

Task	Description	Silver	Gold	Platinum
Ingest Data from Log and Event Sources*	Support the ingestion of data from a range of technologies and services as log and event sources as provided by NTT from time to time. Monitor log feed for log ingestion failure.			
Data Retention	Retain Analytics Logs for in scope devices for ninety (90) days from the date of transmission to NTT. Retain Alert and Incident data for 18 months from the date of creation.			
MDR Incident Detection	Provide 24 x 7 MDR incident detection. Alerts created by the MDR platform, based on the severity of the alert a ticket will be logged in NTT ITSM with a notification to Client, upon NTT's determination in its sole and absolute discretion that an alert requires a ticket.			
MDR Incident Report	Provide Client with a MDR Incident Report that includes a detailed description of the threat, identified activity combined with a recommendation of suitable incident response steps to take. Further updates to the MDR Incident are updated on the Services Portal.			
Information Security Manager (ISM)	Provide a subject matter expert in cyber security, with a strong operational focus ensuring value realization of the MDR service. The ISM supports Client as part of a long-term relationship which enables the ISM to develop a deep understanding of the Client's environment and business. ISM support includes: <ul style="list-style-type: none"> MDR incident escalation point Major incident support between NTT and the Client Optimization recommendations 			
Monthly Service Report	Provide Client with a monthly service report which include extracts from Sentinel Workbooks, Services Portal Widgets, and ITSM incident summary.			
Monitoring	NTT shall monitor the health of deployed system components using native and 3rd party tooling,			

	<p>which shall include at a minimum heartbeat functionality of the agent installed on syslog forwarders in order to ensure at regular intervals of at least every 30 minutes the system is alive (unless otherwise agreed with the Client). In the event that NTT becomes aware of downtime or other technical issue which adversely affects NTT's ability to deliver the In Scope services within Client's Azure subscription or on other Client managed infrastructure NTT shall make commercially reasonable efforts to notify the Client Contract Executive.</p>			
Response Action	<p>A Response Action will be performed if the following are met:</p> <ul style="list-style-type: none"> • The technology that requires the Response Action has the capability of NTT performing the action; • NTT has been granted the appropriate access by the Client; • Client has completed the required consent and documentation; and • NTT has detected an MDR Incident in its' sole and absolute discretion that requires a Response Action. <p>Otherwise, all Response Actions are out of scope.</p> <p>A Response Action for a Client under this Service Description shall be limited to restriction on the flow of traffic through a device which manages traffic through the environment.</p>	✓	✓	✓
Digital Forensics and Incident Response	<p>Provide up to twenty-five hours of DFIR support per contract year, which includes the following:</p> <ul style="list-style-type: none"> • 24 x 7 on-call service • 4-hour Contact Response • Provide remote support and coordination with security and/or IT staff and management to accomplish incident response activities • Provide expert guidance on eradication and recovery • Correlation analysis across various supported and unsupported log sources • Evidentiary compliant handling with chain of custody • Forensic data storage up to 30 days, which shall be in one of the following: Australia, America or the United Kingdom. • Expert digital forensic imaging and analysis on most platforms including mobile, at NTT's sole and absolute discretion • Memory forensics • Review and analysis of various Attack Sensing and Warning (ASW) technologies and related log and network data applicable to the active threat in the environment • Malware reverse engineering • Provide final DFIR report including timeline and analysis findings and recommendations • NTT may provide endpoint detection response tools temporarily to support DFIR investigative activities upon 	✓	✓	✓

	agreement of any required End User License Agreements.			
Use Case Tuning	Tune existing Use Cases for supported sources, to reduce false positives, based on emerging threats, updates to the watchlist and results from threat hunting.	✓	✓	✓
Quarterly Service Review Meeting	Client meetings with ISM to review monthly reports and discuss overall service performance and discuss additional features and roadmap for client.	✗	✓	✓
MDR Incident Management	24 x 7 security analysts validate and investigate threats, suspected threats and notify Client through the Services Portal. NTT may contact Client by telephone for Severity 1 or Severity 2 MDR Incidents. Where applicable, the security analyst will initiate a Response Action.	✗	✓	✓
Check Event Distribution	Compare data source event distribution against historical trends. Associate specific changes linked to seasonal events. Identify risk impact on the Client and provide the ISM with a breakdown of the events.	✗	✓	✓
Threat Hunting	Security analyst proactively and iteratively search through logs to detect and isolate advanced threats that evade existing use cases and existing security solutions using threat intelligence data.	✗	✓	✓
Custom Use Case Tuning	Create Client custom detection rules (up to 10 per year) for specific cases based on Client requirements as deemed reasonable by NTT in its sole discretion.	✗	✗	✓
Targeted Threat Hunting	Investigate and identify patterns on data collected for a specific industry or region (up to 24 per year and no more than 2 per month). Security Analysts review and analyze logs in the LAW and conduct comparisons against new threats and industry specific threats, hunting for any anomalies in a client's environment.	✗	✗	✓
Update Special Handling Notes	Quarterly update special handling notes for Client Security Incident Notification and Management.	✗	✗	✓

*The table below defines the data ingest packages available within the MDR Service. The Client selected data ingest package is detailed in the Fees section of the SOW.

Data Ingest Packages	Daily Ingest (GB)
Small	<50 GB
Medium	<100 GB
Large	<250 GB
X-Large	As specified in the SOW.

5 NTT Service Portal

The MDR system integrates with the provided NTT Services Portal and allows the Client to view interrogate and leverage MDR dashboards and MDR incident reporting. Select dashboards, information and alerts may be linked to or provided within the Client Azure Tenant. NTT reserves the right to update the NTT Services Portal and provide additional functionality in the future using either the Client Azure Tenant or a Third Party Provided Application which shall provide at least substantially similar or enhanced functionality.

6 Optional Extended Log Management Services

Client must expressly select Extended Log Management Services in the SOW as in-scope otherwise they are expressly out of scope.

- (a) Log Analytics Workspace Data Retention up to two years.
- (b) Log Analytics Workspace Data Archive up to seven years.

7 Information Security Management

7.1 Information Security Management is a component of NTT's Managed Detection and Response (MDR) Service delivered by a designated individual. The key functions of Information Security Management include:

- (a) Interpret MDR security information potentially to identify trends and make recommendations.
- (b) Support appropriate business, security, and technical reviews as part of the regular Service Management cadence as detailed below in Coverage.
- (c) Support for Severity 1 and Severity 2 MDR Incidents and provide recommendations on response options up to the provided limits Coverage section.

7.2 The primary responsibilities of the Information Security Manager (ISM) include:

- (a) Advise on service optimizations through additional log sources, feeds and intelligence as required to maintain Client service quality.
- (b) Communicate any changes in Client environment/network that will impact the MDR service.
- (c) Perform reviews of the MDR service against Client security objectives annually.
- (d) Function as final escalation point for technical service-related issues and MDR Incidents requiring additional support after the standard ticket process has been followed.
- (e) Engage with other NTT security teams as required (e.g., MDR Incident Response, Digital Forensics and Incident Response, Cyber Threat Intelligence and Threat Vulnerability Management).
 - (i) Review alerts and advisories from NTT and other Threat Intelligence sources to determine the applicability of the vulnerability to Client's environment and provide advice on actions.
 - (ii) Provide potential security insights and recommendations based on evolving threats.
 - (iii) Form part of escalation team for technical escalations during Business Hours.

7.3 Coverage

The availability of Information Security Management (ISM) is subject to applicable locations and shall be the local time zone the Registered Office location of the SOW Signatory of the Client, unless otherwise specified in the SOW.

(a) ISM Tasks included in the Silver Service Tier

Task	Description	Frequency	Limitations/Out of Scope
Service Delivery Reports	Provide security and technical input to monthly reports required for service delivery.	Monthly	Standard reports only
Client Major Security Incident Management Support	Provide a technical point of escalation for major security incidents identified by the service or escalated and declared by the Client with the Major Incident Management processes operated and managed by the Client.	As needed	During Client local business hours
Service Optimization	Provide expertise to support the optimization of service delivered to Client, working with teams on rule improvements, notification simplification and technical advisories.	As needed	No Client customizations

(b) ISM Tasks Included in the Gold Service Tier

All of the above tasks included in *Silver*, plus the following:

Task	Description	Frequency	Limitations/Out of Scope
Proactive Solution Health-check	Validate service inputs, confirm efficacy of systems, rules, alerts and outputs against Client business requirements.	Monthly	

Service Improvements and Recommendations	Improvement or recommendations of additional log sources that will provide additional benefit to the Client service based on business requirements.	Monthly	
Security Incident Management	Support Client on security incidents requiring additional expert help from security teams.	As needed	
Service Delivery Reviews	Support monthly service review with the Service Delivery Manager to provide security expert support.	Monthly	All shall be provided remotely
Technical Security Service Analysis	Identify potential technical improvements in the service that can be applied within the bounds of the procured service tier. Recommend additions or updates and, if required, suggest next service tiers as appropriate.	Quarterly	All shall be provided remotely

(c) ISM Tasks Included in the Platinum Service Tier

All of the above tasks included in *Silver* and *Gold*, plus the following:

Task	Description	Frequency	Limitations/Out of Scope
Custom Use Case Tuning	Work with Client to tune any included custom use cases from the Service.	Monthly	Maximum 5 use cases per month
Targeted Threat Hunting Support	Work with Client and security teams to define scenarios for targeted threat hunting. Work with investigating teams on active threat hunts by providing Client-specific knowledge and expertise.	Monthly	
Service Delivery Reviews	Attend monthly service reviews with the Service Delivery Manager.	Monthly	Option for on-site support with additional costs.
Detailed Threat Insights Report	Provide detailed security reports to include: <ul style="list-style-type: none"> • Industry insights • Threat landscape information • Risk assessment based on detailed analysis based on anomalies detected in the reporting period • Security insights • Updates on current incident notifications • MITRE mapping of controls and efficacy versus Client targets • Innovation recommendations 	Monthly	

8 Supported Devices for Log Ingestion

NTT maintains a MDR Supported **Technologies** list for log ingestion which may be updated from time to time by NTT. As part of this Service, only technologies in this list can be supported.

9 Limitations

Response actions can only be performed against supported and in scope technologies, which may be updated by NTT from time to time.

The twenty-five hours of DFIR incident response that expire at 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. The Client may elect to use unused unexpired DFIR hours for (or as a contribution towards): Incident Response Plan development, Incident Response Plan gap assessment, Incident Response plan testing, Digital Forensics and Incident Response training or Compromise assessment.

10 Out of Scope

- Standard Security Services as defined in Client Service Description - Security and Compliance do not apply and are out of scope
- Any activity not specified as in scope.
- Any remediation activities post isolation or containment.

- (d) Any DFIR investigation that exceeds the included 25 hours.
- (e) Configuration of any Client devices.
- (f) Consumption of customized log sources.
- (g) Development of customized rules or use cases.
- (h) Creation and presentation of customized reporting.
- (i) Individual Device (Policy) Management.
- (j) Continuous management of Client incidents including coordination of third parties.
- (k) Any device not listed on NTT's supported device list as updated from time to time.

11 Tasks Included in the Standard Transition

As part of the Service, the following tasks are included within the setup fee:

- (a) Assign ISM and SDM for the Client and assign to delivery team, if applicable as specified in the SOW.
- (b) Coordinate with Client to schedule the Project Kick-Off Meeting.
- (c) Verify the Client is configured appropriately within each service-dependent system (MS Azure, ServiceNow, CMDB, Nebula, CI/CD, etc).
- (d) Add Sentinel, Log Analytics Workspace, LogicApps, Syslog Forwarder and other required Security products to MS Azure subscription.
- (e) Apply default Project Artifacts (workbook templates / playbooks / analytics rules from CI/CD).
- (f) Provide Client access to MS Azure and guidance for onboarding log sources.
- (g) Confirm all expected log sources are online.
- (h) Perform Normalization and Tuning and any Pre-Go-Live checks.
- (i) Handover to SOC and Service Commencement on agreed date.

12 Tasks not Included in the Standard Transition

The following tasks are not included in the standard transition:

- (a) Setup and configuration of any technology or third-party service not in scope of the Services.
- (b) Setup and configuration of any technology or third-party service not defined specifically within Client supplied in scope sources and assets.
- (c) Any setup and configuration of any technology or third-party service that requires physical access to the log source or assets to complete the deployment tasks.
- (d) Any setup and configuration of any technology or third-party service not on NTT's MDR Supported Technologies list as updated from time to time.

13 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 MDR 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 daily ingest threshold in scope in the SOW for three days in a single month, NTT reserves the right to change Client ingest package. NTT shall make commercially reasonable efforts to notify the Client when the Client has exceeded the ingest package.
- In any month that the Client exceeds the daily ingest threshold in scope in the SOW, no Service Level penalties shall apply.
- Client expressly agrees to:
 - Prevent unauthorized access to or use of Services and notify NTT promptly of any such unauthorized access or use;
 - Use the Services only in accordance with this Service Description, the Documentation, the SOW, Contract, and the Agreement;
 - represent and warrant the accuracy, quality and legality of Client Data, the lawful means by which Client acquired Client Data, and Client's right to use Client Data with the Services;
 - represent and warrant (i) the provided IP addresses and In Scope Devices and any other devices functioning at those IP addresses are owned or controlled by Client, and (ii) Client has the right to authorize Supplier to access the IP addresses and devices in providing the Services;
 - not sell Client resell, sub-license, sell, distributes, or transfer the use of the Services to any other party; and
 - consent to NTT (a) retaining archival copies of work product and (b) using and disclosing general statistics and non-identifiable information regarding vulnerabilities and security issues.
- Client expressly agrees that NTT may perform actions that are related to operation of the Services which may result in increased costs for Clients Azure services, including but not limited to, search jobs and data restores on log data, running playbooks, and changes to ingest configuration.
- NTT shall only be responsible for security to systems and Client Data upon which NTT has sole access and control. NTT shall not be responsible for any Client Data stored on Client systems, transmitted to or from third parties, or processed by any third party.
- 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 waives all claims for any and all damages related to that activity.

- Client is responsible for backing up all Client Material and Hosted Data. Log files and Sentinel content (including but not limited to workbooks, playbooks, and analytic rules) stored as part of the Service will be immediately deleted by NTT on termination of the Services, and these shall not be returned to the Client, unless log storage has been purchased as a service and specified as in scope in the SOW or as mutually agreed as part of the Transition Plan during Termination Assistance. No retention of any Client Materials or Client Data shall be included in this SOW, unless specifically included as in-scope and only for the specific time period and data types specified. Further, any Sentinel content (including but not limited to workbooks, playbooks, and analytic rules) shall be deleted from the Client Azure subscription, and Client shall assist with this activity. Client shall have no use rights after this Service is terminated and Client must ensure that no NTT confidential or proprietary material remains in its possession.
- 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.
- MDR Incident shall mean an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies for a Client System connected to the MDR Platform by providing an ingestion feed.
- A MDR Report shall mean a report based on an MDR Incident.