Managed Extended Detection and Response (MXDR)

Overview of the Service

NTT's Managed XDR is a holistic offering securing the enterprise and providing rapid detection and effectively responding to cybersecurity threats, using advanced analytics, threat intelligence, expert-driven threat hunting, automation, and validation capabilities.

Required Operational Technologies for the Managed XDR Service provided by Client:

- Palo Alto Networks XSIAM Base
- Either Palo Alto Networks XSIAM Enterprise or XSIAM Enterprise & Cloud

Optional Operational Technologies for the Managed XDR Service:

- NTT Digital Forensics and Incident Response Retainer (In excess of 25 hours)
- NTT Vulnerability Management
- NTT Device Management
- NTT Managed SASE
- NTT Threat Intelligence Service(s)
- Palo Alto Networks Capacity Add-Ons (Data Retention or Query Capacity)
- Palo Alto Networks Threat Intelligence Platform License
- Palo Alto Networks Attack Surface Management
- Palo Alto Networks Identity Threat Detection & Response
- Managed Prisma SASE

Access Management Requirements:

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

- **Role Assignment:** Client to assign user roles based on their job functions, such as network administrators, security analysts, or auditors. Each role is associated with a predefined set of permissions and access rights which need to be appropriately assigned to NTT resources as requested by NTT.
- The Client to assign Permissions using the Cortex XSIAM Permission Management console as requested by NTT, which is accessible via the Cortex Gateway.

Client Responsibilities

Client must perform the following activities:

- Provide a project manager or other single point of contact ("SPOC") for the project who will be responsible for:
  - Providing all information, as requested by NTT, in a timely manner.
  - Act as the central point of contact to NTT.
  - Coordination of Client resources engaged in the project.
- Be responsible for procurement and upkeep of any and all licenses for any and all Palo Alto Networks Products during the contract of managed service.
- Provide up-to-date documentation including, but not limited to, topological diagrams, design documentation, up-to-date configurations, and change management policy documentation.
- Be responsible for managing all other vendors (excluding NTT), including, if applicable, systems integrators.
- Configure all in scope devices in accordance with the requirements of the Service and NTT instructions, unless specified otherwise in the SOW.
- Ensure all logs from in scope devices, not managed by NTT, are sent to the Managed XDR service platform.
- Provide the underlying infrastructure and manage the up-time of the broker VM(s) and Cortex XSOAR Engine.
- Be responsible for the deployment of Endpoint Detection and Response (EDR) agents within the client environment. NTT will provide the EDR agent for deployment.
- Provide the number of endpoints currently deployed within the client environment and inform the NTT ISM on a quarterly basis.
- Client will provide connectivity API keys to log source and device connection.
- Configure and license virtual machine(s) or servers required for log forwarding or associated services.
- Provide any additional equipment, such as network analyzers, test equipment, and/or laboratory equipment not provided by NTT, but necessary to perform the Services.
- 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.
- Client must comply with NTT's MXDR Supported Technologies list for ingest, which may be updated by NTT from time to time.
- Client must complete a Response Action Agreement before NTT will perform any 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.
- Client will provide NTT a list of acceptable and authorized tasks in a form acceptable to NTT, in the event Client does not provide a list of acceptable and authorized tasks, no isolation activities will be performed. Any updates to this list must have 30 days written notice.
- Client will be responsible for maintaining an authorized list of users and/or a distribution list for notification of MXDR Incidents detected by the MXDR service. Client will be deemed to have accepted notification of an incident upon NTT's notification to the agreed recipients.

Sensitivity Label: General

- Ensure that NTT personnel may access and use Client's and third-party licensors' proprietary materials as necessary for NTT to perform the service. Client warrants and represents that it has the right and authority to grant such access and use to NTT and hereby grants NTT the rights to use and access such proprietary materials as needed for NTT to perform the Services.
- Client agrees to have read only access to the XSIAM platform while under the management of NTT MXDR service.
- Upon notification of an MXDR Incident by the MXDR service, the Client is responsible for further (beyond NTT initial analysis) activities associated with triage, investigation, and security incident management in accordance with the recommendations provided by NTT in the MXDR.
- Where NTT is responsible for operational management of Cortex XDR agents which requires remediation as part of the security incident or MXDR 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 Agent.
- Where NTT is responsible for operational management of Configuration Items (CI) which requires remediation as part of the security incident or MXDR 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.
- 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).
- Client is responsible for any impact to any NTT SLAs, due to the use of Client procured third party security tools during an incident or investigation.

Service Specific Operations

NTT offers three service levels for Managed XDR. The service level must be selected as In Scope in the SOW, otherwise all are out of scope.
Tasks legend:

- Tasks marked as ✓ are included in the service for the specified level.
- Tasks marked as ✗ are not included in the service for the specified level.

Task	Description	Silver	Gold	Platinum
Data gathering and project Kickoff	Gather information related to the Client requirements, assets and scoping the solution aligned to Client requirements which may only be performed once	✓	✓	✓
Platform Deployment Management	Deploy and Configure the XSIAM management platform and components which may only be performed once	✓	✓	✓
Agent and log forwarder Deployment Management	Support in the deployment of the XDR & EDR agents, log forwarders and perform testing to ensure data is correctly being received into the MXDR platform. Provide the client with the EDR agent (license provided by Client) and liaise with the client to enable the agent to be uploaded to the Client's software distribution tool (Intune / SCCM (Microsoft Endpoint Configuration Manager (MECM)) as example) for the client to deploy.	✓	✓	✓
Ingest Data from Log and Event Sources*	Support the ingestion of data from a range of supported technologies and services which maybe updated from time to time. Monitor log feed for log ingestion failure.	✓	✓	✓
Data Retention	Retain ingested raw data for 30 days within the XSIAM platform, alert and incident data for 180 days and forensic data for 90 days. Data storage is only applicable for devices that are in scope. Incident and alert data are retained according to the last Update Date and Creation Date, respectively.	✓	✓	✓
System Monitoring	NTT shall monitor the health of deployed NTT system components using native and 3rd party tooling, 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 Palo Alto XSIAM subscription or on other Client managed infrastructure NTT shall make commercially reasonable efforts to notify the Client	✓	✓	✓
Incident Detection	Provide 24 x 7 incident detection and endpoint detection generated by the XDR agent on the device. Alerts created by the Managed XDR platform	✓	✓	✓

Sensitivity Label: General

	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.			
Endpoint Detection & Response Policy Management	Utilize the pre-defined EDR policies that are included within the XDR platform to control the behavior of the agent on each device providing a more tailored EDR experience aligned to the Client requirements. Maintain and configure EDR policies and exclusion policies for specific assets and applications upon reasonable Client request up to NTT's reasonably determined limits. Work with the Client to provide ongoing optimization and policy changes to reduce the number of false positives.	✓	✓	✓
Response Action	A Response Action will be performed if the following are met: · 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 MXDR Security Incident in its' sole and absolute discretion that requires a Response Action. Otherwise, all Response Actions are out of scope. 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. Response Action means an action taken by NTT in response to an analysist confirmed MXDR Security Incident that impacts a Client system.	✓	✓	✓
Endpoint Remote Isolation	Perform remote actions for isolation of compromised / malicious hosts following security analyst validation only for Endpoints with the Cortex XDR agent installed and managed and in accordance with the acceptable task list provided by Client	✓	✓	✓
Digital Forensics and Incident Response	Provide up to twenty-five hours of DFIR support per contract year, which includes the following: · 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. · 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	✓	✓	✓
Standardized Playbooks	Activation and deployment of playbooks that are provided within the XSIAM technology stack enabling incident detection, response and remediation automation.	✓	✓	✓

Sensitivity Label: General

MXDR Incident Management	24 x 7 security analysts validate and investigate threats, suspected threats and notify Client through the Services Portal. NTT may notify a Client by telephone or Microsoft Teams for Severity 1 or Severity 2 MXDR Incidents only. Where applicable, the security analyst will initiate a Response Action.	✓	✓	✓
MXDR Incident Report	Provide Client with an Incident Report that includes a description of the threat, identified activity combined with a recommendation of further incident response steps to take. Further updates to the 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 Managed XDR service. The ISM supports Client as part of a long-term relationship which enables the ISM to develop an understanding of the Client's environment and business. ISM support includes: · Managed XDR incident escalation and communication point · Major incident support during ISM's business hours between NTT and the Client	✓	✓	✓
Monthly Service Report	Provide Client with a monthly service report which may include: · Overview of service status, SLA compliance, high risk observations and trends within the client environment. · EDR compliance reports and remediation recommendations Additional security services recommendations aligned with the client's threat profile.	✓	✓	✓
Portal Access	Client access to a unified portal that will act as a single interface point enabling for example security incident reports, ticket management, document sharing etc.	✓	✓	✓
Threat Hunting	NTT Threat Hunters will search through the ingested logs to detect and isolate advanced threats. This threat hunting is triggered by a security incident, threat intelligence or a new security advisory.	✓	✓	✓
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.	✗	✓	✓
XSIAM Addon Modules	Provide additional managed service capabilities for XSIAM addons which include; Threat Intelligence Management and Digital Forensics and Incident Response at an additional cost and all licenses must be provided by the Client.	✗	✓	✓
Notification & Detection Playbooks (Gold)	Create and deploy up to 10 customized playbooks per year for supported sources, detection alerts, reduce false positives, based on emerging threats, updates to the watchlist and results from Threat Hunting as deemed reasonable by NTT in its sole discretion.	✗	✓	✗
Targeted Threat Hunting (Gold)	Upon client request, investigate and identify patterns on data collected for a specific industry or region (up to 10 per year and no more than 2 per month). Security analysts review and analyze log data and conduct comparisons against new threats and industry specific threats, hunting for any anomalies in a client's environment upon client request.	✗	✓	✗
Notification, Detection and Response Playbooks (Platinum)	Create and deploy 20 customized playbooks per year for supported sources, detection alerts, reduce false positives, incident response based on emerging threats, updates to the watchlist, results from threat hunting and threat intelligence.	✗	✗	✓
Targeted Threat Hunting (Platinum)	Upon client request, 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 log data and conduct comparisons against new threats and industry specific threats, hunting for any anomalies in a client's environment upon client request.	✗	✗	✓

Phishing Protection	Provide detection and alerting of domains involved in phishing email campaigns, client look-alike domains and subdomains that can be used deceive online users and notify the client.	✗	✗	✓
Domain Monitoring	Monitor, analyze and alert the client to registered domains that impersonate a client that could be used in a malicious attack against the Client	✗	✗	✓
Threat Intelligence – Sector Reporting	Generate threat report by pulling Threat alerts, Threat Actor updates & TTPs, and significant events that may impact the Client	✗	✗	✓
Attack Surface Management	Monthly threat exposure reporting that contains prioritized threat scores of risky client assets, automated resolutions (via playbooks) and benchmark against other organizations*. ISM meeting to run through and contextualize the threat report in conjunction with the client risk appetite and security posture prioritization.	✗	✗	✓

***Playbook Defined:** a series of tasks, conditions, automations, conditions, commands, and loops that run in a predefined flow to save time and improve the efficiency and results of the investigation and response process.

Attack Surface Management (ASM) (Platinum Clients Only)

The management of Palo Alto Network's Attack surface management solution is included at no extra cost for Platinum clients. The client is responsible for acquiring the license from Palo Alto before any management services can be deployed.

Task	Description	Silver	Gold	Platinum
Digital Asset Library	Provide accurate inventory of clients digital assets and provide a report including what is connected to the network, where it is located, and its current state.	✗	✗	✓
Un-associated Responsive IPs	Provide a list of IP addresses that may pose a security risk but are not yet linked to specific assets.	✗	✗	✓
Asset Certifications	Identify certificates attributed to the Clients organization and whether the certificate advertised recently, misconfigures or up for renewal.	✗	✗	✓
Organizational Domains	Provide a list view of all domains that attributed to the Client's organization and whether each domain has a recent resolution.	✗	✗	✓
External Services	Provide an inventory of all of the public internet-facing services attributed to the Client's organization. An external service can be any internet-facing device or software that communicates on domain:port or IP:port pair.	✗	✗	✓
External IP Address Ranges	Provide external IP address ranges enabling the Client to understand threats originating from outside the organization	✗	✗	✓
Managed & Unmanaged Asset Identification	Discover externally exposed cloud services running on the known IP space of various cloud providers. Ability to discover a service NTT is confident belongs to the client but was unable to find any assets present in Prisma Cloud to correlate with this service. This means that there is an asset/service exposed to the public internet that is seemingly unmanaged.	✗	✗	✓
Shadow Cloud Detection – Domains	Closely observe domains linked to a client's organization that resolve to IP addresses associated with cloud-based services. This insight allows NTT to recognize the presence of cloud services used by a Clients organization.	✗	✗	✓
Shadow Cloud Detection – Certificates	Discover certificates that are attributed to the client and are observed on services discovered on cloud IPs. NTT notes these certificates when they are observed on services hosted on cloud IPs, further expanding its understanding of the cloud infrastructure's impact on security.	✗	✗	✓
Monthly Reporting	Aggregate and summarize monthly trending insights into a single report, enabling the Client to: · Maintain a continuously up-to-date inventory of all internet-connected assets. · Identify Cloud and On-Premises assets that do not comply with company policy. · Prioritizing exposures for remediation based on risk.	✗	✗	✓

Sensitivity Label: General

	· Track digital assets like IP addresses, certificates, domains, and their registrations. The NTT ISM will conduct monthly sessions with the client to: · Review the Client's overall security posture, with a high-level summary of the providers and region with the highest risk · Analyze the Client's security posture trend over the last 90 days · Discuss the Client's security posture score broken down by business unit, geo-IP location, and hosting provider. · Provide a list of the Client's highest risk incidents, enabling the Client to focus their remediation efforts where they will have the most significant impact.			
Peer Benchmark	Provide a benchmark using the ASM tooling to inform the Client of their security posture vs similar peer organizations and provide prioritized recommendations in improving their score.	✗	✗	✓
Attack Surface Testing	Determines the status of an application vulnerability, benign exploitation of the vulnerability is often required. Attack Surface Testing fills this need by running unintrusive, benign exploits to confirm the exploitability of vulnerabilities on the organization's owned services. Up to 10 tests can be conducted per month.	✗	✗	✓
Alert Tuning	Work with the Client to tune the alerting functionality to the Client's requirement and change the priority scoring of the alerts to the Client risk profile.	✗	✗	✓

*The table below defines data ingest packages which Client will select and is defined in SOW.

Data Ingest Packages	Daily Ingest (GB)
Small	<50 GB
Medium	<100 GB
Large	<250 GB
X-Large	Increments of 250GB to 2TB

NTT Service Portal

The MXDR system integrates with the provided NTT Services Portal and allows the Client to view, interrogate and leverage MXDR dashboards and MXDR incident reporting. Select dashboards, information and alerts may be linked to or provided within the Palo Alto Networks console. NTT reserves the right to update the NTT Services Portal in its sole discretion.

Information Security Management

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

- Interpret MXDR security information potentially to identify trends and make technology, service and/or configuration recommendations.
- Support appropriate business, security, and technical reviews as part of the regular Service Management cadence as detailed below in Coverage.
- Support for Severity 1 and Severity 2 MXDR Incidents and provide recommendations on response options up to the provided limits Coverage section.

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

- Advise on service optimizations through additional log sources, feeds and intelligence as required to maintain Client service quality.
- Communicate any changes in Client environment/network that will impact the MXDR service.
- Perform reviews of the MXDR service against Client security objectives annually.
- Function as final escalation point for technical service-related issues and MXDR Incidents requiring additional support after the standard ticket process has been followed.
- Engage with other NTT security teams as required if the team is in scope (e.g., MXDR Incident Response, Digital Forensics and Incident Response, Cyber Threat Intelligence and Threat Vulnerability Management).
    - 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.
    - Provide potential security insights and recommendations based on evolving threats.

- Form part of escalation team for technical escalations during Business Hours.

Coverage

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

ISM Tasks included in the Silver Service Level

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
EDR Compliance	Provide compliance report(s) on EDR agents deployed and active within the client estate. Highlighting endpoint compliance breach(s).	Monthly	
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

ISM Tasks Included in the Gold Service Level

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

Task	Description	Frequency	Limitations/Out of Scope
Proactive Solution Heath-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
Custom Use Case Tuning	Work with Client to tune any included custom use cases from the Service.	Monthly	Maximum 2 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	

ISM Tasks Included in the Platinum Service Level

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
Atack Surface Management	Provide insights into attack surface management scans that have been conducted within the month	Monthly	
Domain & Phishing Update	Provide details on the malicious domains that have been detection (and taken down if in scope) and provide recommendation insights.	Monthly	Domains that are in scope

Sensitivity Label: General

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: · Industry insights · Threat landscape information · Security insights · Updates on current incident notifications · MITRE mapping of controls and efficacy versus Client targets · Innovation recommendations	Monthly	

Supported Devices for Log Ingestion

NTT maintains a MXDR 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.

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 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.
- NTT will be the sole manager of the XSIAM console and the client will be provided read only access and reporting functionality unless expressly agreed on the SOW.
- Any infrastructure downtime or actions taken by the client that negatively effects the proper function of the VM broker(s) resulting in communication degradation between the client environment and XSIAM will negate any NTT SLA obligations until proper VM broker service is resumed (this is specific to the underlying infrastructure only).
- NTT will support the total number of users as stated within the XSIAM license. The minimum number of XDR agents supported as part this service is 500 per client. Any increase in number of XDR agents will be in multiples of 250 agents (1 XDR agent equals 1 Endpoint).
- NTT reserve the right to confirm the total number of XDR agents supported within the XSIAM console to ensure alignment with the statement of work (SoW) on a quarterly basis. If the total number of XDR agents exceeds what is defined within the SOW, NTT shall have the right in its sole discretion to adjust the pricing based on these changes for the remainder of the Term in the Statement of Work. Endpoint counts cannot be reduced.
- Playbook creation maybe limited by the functionality and compatibility of the XSIAM
- EDR vendor technology supported is limited to PAN XDR, CrowdStrike and Microsoft Defender.

Out of Scope

- Standard Security Services as defined in Client Service Description - Security and Compliance do not apply and are out of scope
- Any remediation or up time support for the Broker Virtual Machine
- Any activity not expressly specified as in scope.
- Any recovery activities post isolation or containment (where DFIR is not enacted).
- Any DFIR investigation that exceeds the included 25 hours.
- Deployment of EDR agents onto client endpoints
- MXDR service does not include further remediation actions post endpoint isolation.
- Consumption of customized log sources.
- Creation and presentation of customized reporting.
- Continuous management of Client incidents including coordination of third parties.
- Any device not listed on NTT's supported device list as updated from time to time.
- NTT supporting any data sources that are not explicitly supported by the Palo Alto XSIAM platform.
- Client edit access rights to the XSIAM platform unless explicitly agreed on the SOW.
- Any transmission, processing, or storage of any data, information or otherwise that requires any license, authorization, certification or attestation

Tasks Included in the Standard Transition

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

- Assign ISM and SDM for the Client and assign to delivery team, if applicable as specified in the SOW.
- Coordinate with Client to schedule the Project Kick-Off Meeting.
- Verify the Client is configured appropriately within each service-dependent system (ServiceNow, CMDB, Nebula, CI/CD, etc).
- Apply default Project Artifacts (workbook templates / playbooks / analytics rules from CI/CD).
- Confirm XSIAM console set up
- Create the EDR agent for client to deploy across endpoint estate

Sensitivity Label: General

- Create High level and low level design documents
- Confirm all expected log sources are online.
- Perform Normalization and Tuning and any Pre-Go-Live checks.
- Handover to SOC and Service Commencement on agreed date.

Tasks not Included in the Standard Transition

The following tasks are not included in the standard transition:

- Setup and configuration of any technology or third-party service not in scope of the Services.
- Setup and configuration of any technology or third-party service not defined specifically within Client supplied in scope sources and assets.
- 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.
- Any setup and configuration of any technology or third-party service not on NTT's MXDR Supported Technologies list as updated from time to time.

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 MXDR 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 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 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 XSIAM services, including but not limited to, search jobs and data restores on log data, 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 represents and warrants all NTT use as allowed under this Service Description, Client's use or any other use of all third party tools, access or software provided by Client (including by not limited to Palo Alto software) shall be in compliance with its license agreements and appropriate use rights. Client shall indemnify, defend and hold harmless NTT from any claim of the preceding.
- Client is responsible for backing up all Client Material and Hosted Data. Log files and XSIAM 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 Further, any NTT IP (including but not limited to workbooks, playbooks, and analytic rules) shall be deleted from the Client's XSIAM 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.
- MXDR 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 MXDR Platform by providing an ingestion feed.
- A MXDR Report shall mean a report based on an MXDR Incident.

Sensitivity Label: General