Managed Extended Detection and Response - Threat Intelligence Add-on

1 Overview of Service

The Managed Extended Threat Detection and Response (MXDR) threat intelligence add-on provides an enhancement to the MXDR.
The services described herein are in addition to the MXDR Services described in the Managed Extended Detection and Response Service Description. MXDR Threat Intelligence is not a standalone service and is only in scope if Managed Extended Detection and Response has also been contracted and is in scope.

In addition to services included in MXDR, MXDR Threat Intelligence service may provide, depending on the selected services which must be specified as in scope in the SOW:

(a) Palo Alto Threat Intelligence Platform Management

(b) Brand & Domain Monitoring plus Takedown

(c) Digital Risk Protection Service

(d) Tailored Threat Intelligence

(e) ThreatMatch Platform Access

1.2 Required Operational Technologies for the Managed XDR Threat Intelligence Service

(a) Managed Extended Detection & Response Gold or Platinum Service

2 Client Responsibilities

(a) Provide a single point of contact (“SPOC”) for the project who will be responsible for:

(i) Providing all information, as requested by NTT, in a timely manner.

(ii) Act as the central point of contact to NTT.

(iii) Coordination of Client resources engaged in the project.

(b) Be responsible for procurement and upkeep of any and all licenses for the Palo Alto Networks products during the contract of managed service.

(c) Provide up-to-date documentation including, but not limited to: domains, external IP ranges, logos, official social media sites pages, official code repositories and a critical third party supplies. Provide updates as and when required.

(d) Client must sign the domain takedown letter of authority for malicious domains to be taken down automatically. In the event, no takedown letter is completed by the Client and accepted by NTT, no Response Action will be taken by NTT.

(e) Be responsible for managing all other vendors (excluding NTT), including, if applicable systems integrators.

(f) Client will be responsible for maintaining an authorized list of users and/or a distribution list for notification of threat intelligence alerts detected by the service. Client will be deemed to have accepted notification of an alert upon NTT’s notification to the agreed recipients.

(g) Upon notification of a threat intelligence alert by the service, the Client is responsible for further (beyond NTT initial analysis or automatic takedown activities if in scope) activities associated with triage, investigation, and alert response in accordance with the recommendations provided by NTT in the threat alert / report. *This is specific to the Client’s risk appetite and the overall impact to client environment based the clients risk analysis and assessment programme*

(h) Client will log Requests for Information (RFI) to NTT for the ability to task Cyber Threat Intelligence (CTI) consultants and analysts with intelligence questions.

(i) Annual Threat Assessment (if applicable): Attend a kickoff meeting, provide a verbal overview of the business and written details of the business-critical functions and services. Attend a report delivery call for the presentation of the final delivery.

3 Service Specific Operations

3.1 Threat Intelligence Add-On

NTT offers a single managed service offering for the Palo Alto Network Threat Intelligence module.

Task	Description
Data gathering and project Kick-off	Gather information related to the customer requirements, assets and scoping the solution aligned to customer requirements one time.
Threat Intelligence Platform (TIP) Deployment Management	Deploy and Configure the XSIAM TIP and components
3rd Party Feed Integration	The integration of additional customer provided third party feeds into the TIP (if required)

3.2 Brand & Domain Monitoring Plus Takedown

NTT offers two service levels for Brand & Domain Monitoring Plus Takedown service. 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	Gold	Platinum
Data gathering and project Kick-off	Gather information related to the customer requirements, assets and scoping the solution aligned to customer requirements one time	✓	✓
Phishing Protection	The detection and alerting of domains involved in phishing email campaigns, client look-alike domains and subdomains that can be used deceive online users.	✓	✓
Domain Monitoring	Monitors, analyses and alerts the client to registered domains that impersonate a client that could be used in a malicious attack against the client, its customers or supply chain	✓	✓
Domain Takedown	Manual or automated take down of malicious domains that have been identified as malicious.	✗	✓
Social Media Monitoring	Continuously monitor major social media sites like Facebook and Instagram for brand infringement and provide alerting capabilities.	✗	✓
Malicious Social Media Takedown	Utilize takedown processes to remove malicious social media content that infringes on the clients brand. (pre agreed legitimate social media sites to be provided by the client)	✗	✓
Brand Impersonation Detection	Search and neutralize unauthorized brand affiliations, and rogue applications registered in App Stores globally. Search engine scanning to identify brand affiliations and malicious adverts used to mislead potential clients	✗	✓

3.3 Digital Risk Protection Service (DRPS)

NTT offers two service level for the DRPS offering. The service level 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 level.

(b) Tasks marked as ✗ are not included in the service for the specified level.

Task	Description	Gold	Platinum
Leaked Data Detections (Gold)	Identify leaked data across the surface, deep and dark web (Monitor up to 100 domains and 5 brand names)	✓	✗
Credential Monitoring	Identify clients leaked credentials (passwords and / or usernames), provide alerting capabilities to enable Client credential resets.	✓	✓
Social Media Data Leakage	Monitor the client's social media presence for malicious use or brand infringement and inform the client.	✓	✓
Code Repository Leakage	Monitor all official code repositories for detected leaks and provide alerting capabilities to the client.	✓	✓
Deep / Dark Web Monitoring	Provide monitoring capabilities across the surface, deep and dark web. Monitoring capabilities cover; social media, typo-squatting, messaging platforms, dump & paste sites, search engine adverts, data breaches and news & blog channels.	✓	✓
3rd Party Breach Notification (Gold)	Monitor and provide alerting for a clients critical suppliers (**up to 20**) that have been breached.	✓	✗
Bespoke Alerting, Scoring & Recommendations	Generate bespoke, prioritized reports that detail the specific risks attributed to a client's organization over the month.	✓	✓

Sensitivity Label: General

	Findings are prioritized, and specific recommendations are provided to enable the mitigation / reduce the threat severity.		
Leaked Data Detections (Platinum)	Identify leaked data across the surface, deep and dark web (Platinum 250 domains, 10 brand names)	✗	✓
3rd Party Breach Notification (Platinum)	Monitor and provide alerting for a clients critical suppliers (**up to 50**) that have been breached	✗	✓

3.4 Tailored Threat Intelligence (TTI)

NTT offers two service level for the TTI service. The service level 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 level.

(b) Tasks marked as ✗ are not included in the service for the specified level.

Task	Description	Gold	Platinum
Sector Aligned Threat Alerts	Filtered alerts that are ranked by severity for each client. Each alert contains an overview, severity rating, Traffic Light Protocol (TLP), source, intelligence analysis, assessment and recommendations. Where appropriate Indicators of Compromise (IOCs), associated alerts/profiles and comments are also provided.	✓	✓
Threat Actor Operations	A view of an overall operation by specific threat actors against either an entity, sector or nation.	✓	✓
Threat Actor, Tactics, Techniques & Procedures (TTPs) Updates	Provide an in-depth analysis of threat actors (nation state, organized crime groups, hackers, hacker groups, hacktivists), including their usual tactics, techniques and procedures (TTPs), related tools and malware, incidents and associated profiles.	✓	✓
Cyber Significant activities (SIGACTS)	Provide a view of a malicious event against a specific organization(s), government agency or military department, this includes the: who, what, when, where, and why (5Ws) of attacks related to a cyber incident.	✓	✓
RFI Support	8 hours of direct support monthly through 'Requests for Information' where the Client can request information from CTI consultants and analysts about the provided intelligence under this Statement of Work	✗	✓
Consolidated Threat Reports	Provide a monthly bespoke threat intel report. This report may contain: · Bespoke, organizational specific alerts (brand, leaked creds etc) and documents, · The client's monthly incidents, · The wider threat landscape specific to the client. · What are the threat levels for the client's region and sector. · Provides an overview of the client's threat landscape.	✗	✓
Annual Threat Assessment of Clients threat landscape	An analysis and threat assessment developed via the fusing of threat intelligence and red team techniques. This service develops threat scenarios that can be used to test a Client's organizations defense posture against a real-world attack, linked to specific threat actors targeting a Client's industry vertical within a given geo-location. Red team testing is out of scope for this service.	✗	✓

3.5 Reports

(a) Brand and Domain Monitoring Plus Takedown Reports

Reports Summary	Reports
Alerting Information: *Phishing Protection, Domain Monitoring, Social Media Monitoring*	· Alert information generated upon detection and published on the NTT portal or PAN XSIAM Threat Intelligence Platform[1]. · Phishing Protection & Domain Monitoring alerts will contain; automated alerts of newly registered domain variants, certificate variants, domains containing client's brands. automated updated alerts if/as the threat changes · Alerts for malicious social media sites will contain daily automated alerts of imposter domains infringing the client's brand.

Sensitivity Label: General

	· Alerts for malicious brand impersonation will contain daily automated alerts of imposter apps and adverts infringing the client brand.
Takedown Service	· The domain takedown service and brand impersonation will provide daily automated alert updates confirming take down requested and alert updates until the domain or fake application take down is successful.

(b) Digital Risk Protection Service Reports

Reports Summary	Reports

Alerting Information: *Leaked Data Detection, Credential Monitoring, Social Media Data Leakage, Code Repository Leakage, Deep Dark Web Monitoring, 3rd Party Breach Notification*	• Alert information generated upon detection and published on the NTT portal or PAN XSIAM Threat Intelligence Platform[1].
	• Automated alerts upon detection. Each alert is to contain a severity score assessment and remediation recommendations.
	  ○ Credential Monitoring: Alerts of client Credentials breached and leaked by malware, infostealers, client or 3rd party breaches
	  ○ Social Media Leakage: Alerts of client of brand abuse on Social Media.
	  ○ Code Repository Leakage: Alerts of client leakage via repositories shared via scoping exercise.
	• Leaked data detection provides daily automated alerts of client data (when associated to brand of domain) included in data breaches or for sale.
	• Third party breach notification provides daily automated alerts of client mentions in 3rd party breaches or breaches of 3rd parties on the scoping document.

[1] *Automated Alerts are sent as new threats are detected. This may be multiple times per day or every few days, depending upon cadence of breaches.*

(c) Tailored Threat Intelligence Reports

Reports Summary	Reports
· Sector Aligned Threat Alerts	• Automated Alerts of Threat aligned to or relevant to the sectors the client operates in.
· Threat Actor Operations	• Automated Operation Updates of Threat Actor or Malware Operations that are relevant to the customer or globally significant events
· Threat Actor, Tactics, Techniques & Procedures (TTPs) Updates	• Monthly Alerts to updates in Actor TTPs. • *Continuous Access to Threat Actor Profiles for those who have ThreatMatch Access**
· Cyber Significant activities (SIGACTS)	• Automated Alerts and updates to Significant Events in Region, Sector or Globally Important
· RFI Support	• Ah-Hoc short form reports as requested by the client, specific to their Intelligence Requirements.
· Consolidated Threat Reports	• Monthly Intelligence Report specific to the clients Threat landscape and alerting.
· Annual Threat Assessment	• Threat Assessment of the entities threat landscape • Client specific threat scenarios to be generated utilizing threat intelligence and client specific risk appetite data.

**Client must acquire all three threat intelligence services Brand and Domain Monitoring, DPRS and Tailored Threat Intelligence to gain direct access to the Threat Match portal*

Sensitivity Label: General

4 Supported Feeds for Threat Intel Platform (TIP) Ingestion

NTT will refer to the Palo Alto XSIAM supported TIP integration feed list when onboarding new feeds into the platform. NTT will typically support TI feeds from this list that utilize industry standards such as Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Intelligence Information (TAXII) which may be adjusted in NTT's discretion. As part of this Service, only technologies in this list can be supported

5 Limitations

(a) Automated Take down actions can only be performed against supported and in scope technologies, which may be updated by NTT from time to time.

(b) Detection can only occur against the scoping assets provided by the client

(c) If the domain takedown letter of authority is not signed and or recognized by NTT, no automated takedowns will occur. Alerting functionality for malicious content will not be adversely affected if the document is not signed.

(d) Request for Information (RFI) support is restricted to 8 hours for Platinum clients that have adopted the Tailored Threat Intelligence package. Any additional hours required must be included within the Statement of Work (SoW) or acquired standalone.

(e) Additional TIP feed integration will occur during transition using STIX or TAXII formats, any additional threat feeds that are required to be integrated during the duration of the contract will be charged as a standalone item.

(f) Monthly Threat Assessments are restricted to 5 pages, withing NTT template standards

(g) Annual Threat Assessments are restricted to 10 pages, within NTT standard templates, restricted to the assets in the original scope, mapped to standard enterprise critical functions (or any functions highlighted in the scoping documentation).

(h) Annual Threat Assessment limited to 1 briefing session

6 Out of Scope

(a) Any activity not specified as in scope.

(b) Creation and presentation of customized reporting.

(c) Collection against assets not mentioned in scoping documentation

(d) Collection in all closed forums

(e) Domain takedowns against hosting providers in hostile nations

(f) Take downs where ‘brand infringement’ is challenged

(g) Take downs contested by Freedom of Speech, legal challenges

(h) Code leakage not easily identified as directly associated to the client

(i) Take down of Dark Web / Tor sites

(j) Actor Operations, TTPs or Incidents not known to NTT

(k) RFI requests that could breach applicable laws or ethical standards

(l) Red team exercises as part of the threat assessment and scenario generation

7 Tasks Included in the Standard Transition

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

(a) Coordinate with Client to schedule the Project Kick-Off Meeting.

(b) Apply default Project Artifacts (workbook templates / playbooks / analytics rules from CI/CD).

(c) Integrate third party threat intelligence feeds into the Threat Intelligence Platform (if required)

(d) Perform Normalization and Tuning and any Pre-Go-Live checks.

8 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) Handover to SOC and Service Commencement on agreed date.

9 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.

(a) 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.

(b) Client expressly agrees to:

(i) Prevent unauthorized access to or use of Services and notify NTT promptly of any such unauthorized access or use;

(ii) Use the Services only in accordance with this Service Description, the Documentation, the SOW, Contract, and the Agreement;

(iii) 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;

(iv) 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;

(v) not sell Client resell, sub-license, sell, distributes, or transfer the use of the Services to any other party; and

(vi) 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

(c) All MXDR terms and conditions apply to this Service Description.

(d) Client may not further distribute any reports or other deliverables beyond the intended recipient, license restrictions or confidentiality restrictions provided therein.

(e) Client shall have no access to any API, console or other access.

(f) Client is responsible to ensure that all services herein are in compliance with its Palo Alto Licenses.

Sensitivity Label: General