Client Service Description

Threat Detection Service

01 October 2019 | Document Version 1.5
Client Service Description

T{Subject}hreat Detection Service

NTT contact details
We welcome any enquiries regarding this document, its content, structure, or scope. Please contact:

Bob Gordon - Services Product Portfolio Director - Security, Phone: +1 203 446 4942
NTT Limited
✉️ bob.gordon@global.ntt

Please quote reference (Document Reference Number) in any correspondence or order.

Confidentiality
This document contains confidential and proprietary information of NTT Limited ("NTT"). {ClientFull} ("{Client}"") may not disclose the confidential information contained herein to any third party without the written consent of NTT, save that {Client} may disclose the contents of this document to those of its agents, principals, representatives, consultants or employees who need to know its contents for the purpose of {Client}’s evaluation of the document. {Client} agrees to inform such persons of the confidential nature of this document and to obtain their agreement to preserve its confidentiality to the same extent as {Client}. As a condition of receiving this document, {Client} agrees to treat the confidential information contained herein with at least the same level of care as it takes with respect to its own confidential information, but in no event with less than reasonable care. This confidentiality statement shall be binding on the parties for a period of five (5) years from the issue date stated on the front cover unless superseded by confidentiality provisions detailed in a subsequent agreement.

Terms and conditions
This document is valid until 11 July 2019 and, in the absence of any other written agreement between the parties, NTT and {Client} acknowledge and agree is subject to NTT’s standard terms and conditions which are available on request. NTT reserves the right to vary the terms of this document in response to changes to the specifications or information made available by {Client}. Submission of this document by NTT in no way conveys any right, title, interest, or license in any intellectual property rights (including but not limited to patents, copyrights, trade secrets or trademarks) contained herein. All rights are reserved.

NTT does not assume liability for any errors or omissions in the content of this document or any referenced or associated third party document, including, but not limited to, typographical errors, inaccuracies, or out-dated information. This document and all information within it are provided on an ‘as is’ basis without any warranties of any kind, express or implied. Any communication required or permitted in terms of this document shall be valid and effective only if submitted in writing.

All contracts with NTT will be governed by {Law} Law and be subject to the exclusive jurisdiction of the {Law} courts.
Client Service Description

T{Subject}hreat Detection Service

Document Preparation

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepared:</td>
<td>Paul Asdagi</td>
<td>12 Sep 2018</td>
</tr>
<tr>
<td>Prepared</td>
<td>Mike Oberholtzer</td>
<td>01 Feb 2019</td>
</tr>
<tr>
<td>Prepared</td>
<td>Bob Gordon</td>
<td>05 Jun 2019</td>
</tr>
<tr>
<td>Updated</td>
<td>Sharon Witheriff</td>
<td>07 Jun 2019</td>
</tr>
<tr>
<td>Updated</td>
<td>Bob Gordon</td>
<td>01 Oct 2019</td>
</tr>
</tbody>
</table>

Release

<table>
<thead>
<tr>
<th>Version</th>
<th>Date Released</th>
<th>Pages</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3</td>
<td>05 Jun 2019</td>
<td>35</td>
<td>Internal Draft</td>
</tr>
<tr>
<td>1.4</td>
<td>05 Aug 2019</td>
<td></td>
<td>Internal Draft</td>
</tr>
<tr>
<td>1.5</td>
<td>01 Oct 2019</td>
<td></td>
<td>Rebrand</td>
</tr>
</tbody>
</table>

© 2020 NTT Pty Limited. The material contained in this document, including all attachments, is the copyright of NTT Pty Limited. No part may be reproduced, used or distributed for any purpose, without the prior written consent of NTT Pty Limited. This document, including all attachments, is confidential and use, reproduction or distribution of this document or any part of it for any purpose, other than for the purpose for which it is issued, is strictly prohibited. Uptime® is a registered trademark of NTT.

This document is only a general description of the available Services. The Services to be supplied are subject to change. For each Client, the Services will be as set out in the contract entered into by the Client and NTT. If there is any conflict between this document and the contract, the contract will prevail.
Table of Contents

1. Service Description ................................................................. 6
1.1. Overview ............................................................................. 6
1.2. Service Matrix ..................................................................... 8
1.3. Supported Device List .......................................................... 9
1.4. NTT’s Managed Security Services Portfolio .......................... 10

2. Detailed Service Element Descriptions ............................ 11
2.1. 24/7 Security Operations Center Coverage .......................... 11
2.2. Global Threat Intelligence Center ........................................ 11
2.3. Continuous Threat Intelligence Updates ............................. 12
2.4. Advanced Analytics with Proprietary Machine Learning / Behavioural Modelling .................................................. 13
2.5. Security & Confidence Settings ............................................. 14
2.6. Vendor Integration and Evidence Collection for Key Security 15
2.7. SSH Detailed Security Investigation ...................................... 16
2.8. Automated Security Incident reports ................................... 19
2.9. Security Incident Reports Based on Detailed Investigation and Threat Hunting ......................................................... 22
2.10. Client Access to 90 days of Event and Historical Incident Data 23
2.11. Client Enriched and Aggregated Log Search (Option) ....... 23
2.12. Security Appliance .............................................................. 27

3. Our Approach to Service Operations ............................... 29
3.1. Service Experience ............................................................... 29
3.2. Service Desk ....................................................................... 29

4. Service Management ............................................................. 32
4.1. Service Level Management .................................................. 32
4.2. Change management support ............................................. 33

5. Our Approach to Service Transition ................................. 34
5.1. Objectives of Service Transition ......................................... 34
5.2. Transition Methodology ...................................................... 34
Appendix A  Service Level Agreements ..........................36

List of Figures
Figure 1 – Global Managed Security Service Platform........................................10
Figure 2 – Global Managed Security Service Platform........................................11
Figure 3 – Continuous Threat Intelligence Updates ...........................................13
Figure 4 – Detection Capabilities ........................................................................13
Figure 5 – Analyst Workbench ............................................................................18
Figure 6 – Threat Detection Sample of Automated Incident Report......................22
Figure 7 – Investigator .........................................................................................23
Figure 8 – Investigator Log Searches ...................................................................24
Figure 9 – Investigator Search Filtering .................................................................24

List of Tables
Table 1 – Service Matrix.......................................................................................9
Table 2 – Key Vendors Supported by Threat Detection Services...........................9
Table 3 – Example - SYSLOG (SIEM) vs Threat Detection .................................16
Table 4 – Analyst Workbench Components ...........................................................19
Table 5 – Security Incident Categories ..................................................................20
Table 6 – Minimum Virtual Appliance Recommended Specifications ......................27
1. **Service Description**

1.1. **Overview**

Businesses today are under attack from commercially driven attackers that are highly motivated in targeting specific victims with predetermined objectives.

Using a variety of attack vectors, sophisticated attack techniques and previously unseen vulnerabilities makes these attackers more effective and evasive, able to bypass the traditional security measures used to protect and monitor businesses.

The level of sophistication and evasiveness allows attackers to not only bypass these measures, but also benefit from a longer mean-time to detection and response, which gives attackers significantly more time to act on their objectives in breached environments.

Having threats go unnoticed for a long period of time can result in significant commercial impact including damage to company trust, brand value, loss of intellectual property, and financial penalties and lawsuits.

Understanding that there is no single solution or detection technique that offers complete detection of sophisticated attacks, Threat Detection Services leverage the combined insights and capabilities of monitored sources with that of NTT’s proprietary Advanced Analytics, threat hunting, and threat validation capabilities, delivering insights from the network perimeter to the endpoint.

As threats are identified and separated from large amounts of false-positives typically generated by security technologies, relevant contextual information is gathered and presented to a Security Analyst in the global operational teams or sent to you directly as a Security Incident report.

In the **Threat Detection – Standard Service**, threats with high confidence are sent directly to you in the form of a detailed Security Incident report. This report describes the full extent of the identified Security Incident with general recommendations that enable your Incident Response team to act on the identified activity, reducing the mean time to respond to mitigate the associated risk.
In the **Threat Detection – Enhanced** service suspicious activities and all relevant contextual information are presented to a skilled Security Analyst who engages in threat hunting and threat validation activities to verify the threat and its impact, and to identify additional information associated with the potential breach.

Once verified, the Security Analyst creates a detailed Security Incident report and initiates security incident notifications in accordance with your documented procedures. This notification provides a detailed description of the security incident combined with scenario-specific actionable response recommendations which significantly assist businesses in reducing the time taken to make informed, responsive measures, lowering associated risks.

The Threat Detection Service provides:

- 24/7 Security Operations Center coverage
- Services enhanced by the Global Threat Intelligence Center
- Continuous threat intelligence updates driven by production investigations
- Advanced analytics with proprietary machine learning / behavioural modelling
- Automated Security Incident reports
- Customizable web portal
- Client access to 90 days of event and incident data
- Event driven threat hunting.

**The benefits include:**

- Safeguard your business by gaining complete visibility into activity across the IT infrastructure by bringing all your separate security controls into one pane of glass.
- Better protection of information assets to minimize any impact on business operations and reduce overall security risk.
- Rapid identification, prioritization and response to policy breaches, cyber-security attacks, insider threats and critical security advisories.
- Enhanced risk management through effective incident management, incident escalation and rapid response to outbreaks by dedicated Security Engineers and Security Analysts using advanced SOC toolsets.
- Improved agility by freeing up your internal resources to focus on your core business outcomes and requirements.
Client Service Description

T(Subject)hreat Detection Service

- Access to NTT’s Security Operations Center (SOC) for 24/7 support and escalated engineering.

1.2. Service Matrix

The Threat Detection Services are available in two distinct Service Packages, which consist of a core set of elements such as service transition, and associated Service Elements such as incident management.

The Service Package, selected options and associated service levels are formalized in a Record of Entitlement that forms a part of your Managed Services Agreement.

<table>
<thead>
<tr>
<th>Service Elements</th>
<th>Monitoring Services</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Threat Detection - Standard</td>
</tr>
<tr>
<td>Core Service Elements</td>
<td></td>
</tr>
<tr>
<td>Security Appliance</td>
<td>✓</td>
</tr>
<tr>
<td>Service Transition</td>
<td></td>
</tr>
<tr>
<td>Client Transition</td>
<td>✓</td>
</tr>
<tr>
<td>Detection Types</td>
<td></td>
</tr>
<tr>
<td>Advanced Analytics with proprietary machine learning / behavioural modelling</td>
<td>✓</td>
</tr>
<tr>
<td>Threat Intelligence</td>
<td></td>
</tr>
<tr>
<td>Services enhanced by NTT Global Threat Intelligence Center</td>
<td>✓</td>
</tr>
<tr>
<td>Continuous threat intelligence updates driven by production investigations</td>
<td>✓</td>
</tr>
<tr>
<td>Security Analyst Interaction</td>
<td></td>
</tr>
<tr>
<td>Automated analysis</td>
<td>✓</td>
</tr>
<tr>
<td>Detailed Security Incident investigation by Security Analyst</td>
<td></td>
</tr>
<tr>
<td>Event-driven threat hunting</td>
<td></td>
</tr>
<tr>
<td>Vendor integration and evidence collection for key security technologies(^1)</td>
<td></td>
</tr>
<tr>
<td>Client Notification</td>
<td></td>
</tr>
<tr>
<td>Automated Security Incident Reports</td>
<td></td>
</tr>
</tbody>
</table>

\(^1\) Gathers and analyses evidence data in relation to vendor alerts, such as PCAPs and execution reports.
### Service Elements

<table>
<thead>
<tr>
<th>Monitoring Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Detection - Standard</td>
</tr>
</tbody>
</table>

**Analyst-created Security Incident Reports based on detailed investigation and threat hunting**

**Service Portal and Reporting**

- **Service Portal**
  - ✔
  - ✔

- **Client access to Events (90 days)**
  - ✔
  - ✔

- **Client access to Incidents (lifetime of contract)**
  - ✔
  - ✔

**Service Management**

- **Service Level Management**
  - ✔
  - ✔

- **Service Management Review Meeting**
  - ✔
  - ✔

- **Service Delivery Manager**
  - ✔
  - ✔

- **Service Desk**
  - ✔
  - ✔

**Service Options**

- **[Option] Investigator – Enriched and aggregated log search**
  - ✔

- **[Option] Secure Long-Term Log Storage Management**
  - ✔

- **[Option] On Premises POD**
  - ✔

- **[Option] Vulnerability Correlation**
  - ✔

- **[Option] Proactive Response**
  - ✔

**Table 1 – Service Matrix**

#### 1.3. Supported Device List

Supported devices by vendor for the Threat Detection Services are:

<table>
<thead>
<tr>
<th>Check Point</th>
<th>Cisco</th>
<th>F5 Networks</th>
<th>FireEye</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fortinet</td>
<td>Imperva</td>
<td>Juniper</td>
<td>McAfee</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Oracle</td>
<td>Squid</td>
<td>Symantec</td>
</tr>
<tr>
<td>Unix</td>
<td>Zscaler</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 2 – Key Vendors Supported by Threat Detection Services**

- **Highly Recommended.** Important log sources for highly effective threat detection.
- **Recommended.** Useful log sources for threat detection.
1.4. NTT’s Managed Security Services Portfolio

The NTT portfolio of Managed Security Services help reduce the burden of constant and proactive network monitoring, advanced security analysis, and global intelligence correlation. All of our Managed Security Service offerings are powered by the NTT Global Managed Security Service Platform (GMSSP), combined with our proven combination of people, process and technology.

The portfolio of Managed Security Services consists of:

- **Threat Detection Services.** The Threat Detection Services include Standard and Enhanced Service Packages for advanced detection, investigation, and reporting of security incidents.

- **Enterprise Security Monitoring Services.** The Enterprise Security Monitoring Services include Standard and Enhanced Service Packages for security detection and compliance reporting.

- **Security Device Management Services.** The Security Device Management Services include Standard and Enhanced Service Packages for management of a broad range of security technologies.

- **Vulnerability Management Service.** The Vulnerability Management Service delivers customized vulnerability scanning with a variety of compliance and reporting options.
2. Detailed Service Element Descriptions

2.1. 24/7 Security Operations Center Coverage

The Threat Detection Service is delivered out of multiple Security Operations Centers (SOCs) across the globe. These are manned on a 24/7 basis by Security Analysts with extensive vulnerability and threat detection knowledge and supported by strong technical capabilities of the Global Managed Security Service Platform (GMSSP).

Security Analysts will assist with scan maintenance, troubleshooting, configuration, launching on-demand scans as well as stopping scans, asset maintenance and general service and or reporting questions.

![Globally integrated service delivery model](image)

*Figure 2 – Global Managed Security Service Platform*

2.2. Global Threat Intelligence Center

Clients stand to benefit from the extensive threat intelligence both curated and produced by threat intelligence researchers in the Global Threat Intelligence Center (GTIC).

The Global Threat Intelligence Platform (GTIP) acquires threat intelligence data from over 100 open source and commercial feeds, as well as our partnerships including Recorded Future, Cyber Threat Alliance, Cloud Security Alliance, FS-ISAC, VirusTotal, WaPack Labs, FIRST, Red Sky Alliance, U.S. Department of Homeland Security, and the Microsoft Active Protections Program. GTIP also generates data based on honeypot and NETFLOW sensors deployed around NTT’s networks and security events on our Managed Security Services clients’ networks.
Data within GTIP is processed by GTIC analysts who filter irrelevant data and focus on identifying relevant data that can be used to protect your network. NTT Security’s GTIC is joined in this effort by threat intelligence analysts at other NTT companies, including NTT CERT, who share access to GTIP and its collaboration tools.

GTIC makes the findings of their threat intelligence research and NTT Group collaborations available through the GTIP as part of the Threat Detection – Enhanced Service. This data is continuously processed by the analysis engines and made available as contextual threat intelligence to Security Analysts to enable real-time detection and awareness of emerging threats.

- Global Threat Intelligence Center (GTIC)
- Global Threat Intelligence Platform (GTIP)
- Detection of emerging threats
- Contextual information of emerging threats to support Security Analyst investigation

2.3. **Continuous Threat Intelligence Updates**

Threat Intelligence is continuously curated and propagated into the Threat Detection Services from multiple technical and operational sources in an integrated manner that enables efficient and accurate threat detection.

Threat Intelligence propagation is built into the foundation of Threat Detection Services and are ever changing. Additions are made as technical capabilities and operational capabilities are established, and partnerships and collaborations are initiated.

Product threat data is gathered from the global network of analysis engines monitoring client businesses and NTT Group Networks. As these continuously identify known and unknown threats in specific locations, the threat data is gathered and used to improve the detection logic globally through improving machine learning capabilities, creation of rules, and additions to various blacklists.

As Security Analysts identify and escalate verified threats as Security Incidents within the Threat Detection – Enhanced Service, delivery data is automatically gathered and used for the same purposes.

In addition, dedicated Threat Intelligence Analysts in the Global Threat Intelligence Center monitor the global threat landscape for new threats, trends and advisories. Upon identifying such scenarios, the team engages in threat research activities to identify additions and modifications to the threat detection capabilities, including:

- blacklist additions
- pattern signature modification, or creation
- correlation signature modification, or creation
- Collaboration with data scientists improve machine learning capabilities
2.4. **Advanced Analytics with Proprietary Machine Learning / Behavioural Modelling**

Modern threats utilize techniques with rapidly changing indicators (e.g. source IP address, landing page URLs, file names, file hashes) utilized for detection using traditional pattern and reputation-based techniques.

As a result, modern threat detection services cannot rely solely on traditional detection techniques but must also utilize advanced analytics techniques (including machine learning, advanced correlation, threat behaviour modelling, and threat intelligence) to identify suspicious activities. These techniques enable Threat Detection Services to detect known and unknown threats. An overview of detection capabilities utilized in the Threat Detection Services is presented in the following diagram:

*Figure 3 – Continuous Threat Intelligence Updates*

<table>
<thead>
<tr>
<th>REPUTATION</th>
<th>PATTERN</th>
<th>CORRELATION</th>
<th>BEHAVIOR MODELS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat feeds &gt; URL</td>
<td>String Matching &gt; Regular Expressions</td>
<td>Sliding Windows &gt; State Machines &gt; Batch &amp; Real Time</td>
<td>Kill Chain, Boost, Machine Learning</td>
</tr>
<tr>
<td>IP-Address &gt; Domain</td>
<td>Relatively low computing resource requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Hash</td>
<td>Relatively low computing resource requirements</td>
<td>Applicable to many different types of events</td>
<td>Very accurate detection</td>
</tr>
<tr>
<td></td>
<td>Easy to add/remove entries</td>
<td>Easy to prototype and distribute</td>
<td>Very hard to circumvent</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>90-day state keeping</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Detecting new and previously unseen threats</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Auto-tuning and adapting</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Longer lifecycle</td>
</tr>
</tbody>
</table>

*Figure 4 – Detection Capabilities*
Attacker’s usage of a variety of Tools, Techniques, Procedures (TTPs) reduces the significance of the individual indicators (e.g. source IP, URL to landing page, file names or hashes), and these patterns have left traditional detection capabilities struggling to identify such threats. As a result, today’s security programs are required to use a combination of these traditional methods with the signature-less detection capabilities of advanced analytics.

This combination of detection techniques enables broad threat coverage from usage of static indicators of compromises and robust coverage for evasive and unknown threats using behaviour models and various forms of anomaly detection, ensuring swift and accurate threat detection overage over time.

The combined capabilities span the entire monitored estate to contribute in enabling advanced analytics with full insight into the malicious behaviour of potential threats.

Below are some of the advanced analytics techniques used by the Threat Detection Service. This list of modules in the Service are ever-evolving and to be considered as prime examples:

- Machine Learning (Threat Classifiers, Threat Behaviour Models)
  - Threat Behaviour Modeling
  - Cyclic Behaviour
  - Access Anomaly Detection
- Kill-Chain
- Correlation
  - Signatures (over long periods of time >60 days)
  - Boost Scoring (combination of multiple suspicious activities increase EOI)
- Pattern Matching (black lists, reputation, threat intelligence, regular expressions)
- Asset Detection (passive asset discovery and function)
  - Role Based Baselines
  - Suppression of Events
  - Relevance and Context

Usage and availability of each detection technique differs per source-type

### 2.5. Security & Confidence Settings

TD-S uses Machine-Learning in identification and reporting of Security Incidents. As NTT gains knowledge of emerging/or evasive threats, the Confidence in accurately identifying these increases over time. Once Confidence has reached levels deemed suitable for automated service delivery, TD-S will start notifying Clients for matching activity.
While using default Severity and Confidence settings is suitable for most Clients, NTT allows Clients with specific needs to adjust the minimum Confidence level for which suspicious activity will be deemed a Security Incident and the Client notified.

The minimum Confidence levels are set on a Per-Severity basis (Low, Medium and High), example:

<table>
<thead>
<tr>
<th>Severity</th>
<th>Min. Confidence (&gt;=)</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Medium</td>
<td>Max</td>
</tr>
<tr>
<td>Low</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Altering the Confidence level setting increases, decreases, or disables the service’s ability to detect emerging, and evasive threats for the benefit/trade-off of increasing, or decreasing the number of False-Positives, on a per Severity basis.

Severity and Confidence settings are configured during:

- Service Transition described in section ‘4 Service Transition’, by capturing desired configuration in the CSSD.
- Continuous service delivery using Self-Service functionality on the Security Portal.
- Continuous service delivery by submission of a request on the Security Portal.

2.6. **Vendor Integration and Evidence Collection for Key Security**

The Threat Detection Service has established deep integration with multiple supported vendors and technologies to enable collection of evidence data and contextual information beyond standard syslog outputs.

This additional evidence (e.g. PCAPs, Malware Execution reports, host recordings, files, and signature information) not only describes that something suspicious has happened, but also provides significant additional insights into identified threats.

This additional evidence greatly enhances the Security Analyst’s ability to validate the threat, support threat hunting activities, and gain a better understanding of the threat’s potential impact.

This evidence data can be anything from a TCP packet as part of a PCAP trace, to a detailed listing of IOC’s and behavioural information in a Sandbox Executional report, to gigabytes of data in an endpoint recording. Evidence data is made available to the Security Analyst in a proprietary Analyst Workbench, enabling the
Security Analyst with the ability to perform security incident validation and threat hunting.

<table>
<thead>
<tr>
<th>SYSLOG event (typical output stored in a SIEM)</th>
<th>Same event, now combined with PCAP data from the Threat Detection Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-12-08T21:35:09;83.123.221.23; 80; 192.168.10.10; 23491; virus; 191338785; Trojan/Win32.docdl.ltl; allowed</td>
<td>2017-12-08T21:35:09;83.123.XXX.XX; 80; 192.168.10.10; 23491; virus; 191338785; Trojan/Win32.docdl.ltl; allowed</td>
</tr>
</tbody>
</table>

**Table 3 – Example - SYSLOG (SIEM) vs Threat Detection**

The method of integration differs for each vendor to reflect the capabilities and method of making such evidence data available for extraction (refer to device specific solutions guide for specifics). Typical methods, i.e. Integration point (examples) include:

- API (preferable)
- HTTPS
- Streaming
- Database

### 2.7. SSH Detailed Security Investigation

Security events qualified by the analysis engine (or that of reliable signatures triggered by monitored technologies), are presented to the Security Analyst team within the proprietary Threat Hunting and Threat Validation framework called, Analyst Workbench.
Within this framework the Security Analysts are provided with all the information of the event, the holistic insights across customer monitored sources, and strong threat hunting and validation capabilities across these.

- Threat Hunting – Analyst Workbench, Big Data
- Incident Validation – Analyst Workbench, Threat Intelligence, Malware Lab, All Historic Incidents

2.7.1 Even-driven Threat hunting

Security Analysts perform event-driven threat hunting activities as part of security incident validation in the Threat Detection Services. Leveraging the proprietary Analyst Workbench toolset, Security Analysts gain full insights of your monitored sources, as well as contextual information and evidence data in one single-pane of glass.

Enabling not only the ability to follow a threat throughout its life-cycle, but also to hunt for additional activities and lateral movement possibly not detected by any of the monitoring capabilities in place, this is critical in understanding the extent of identified threats and the potential impact.

When examining an alert that has triggered in your environment, the Security Analyst has two objectives: investigate and confirm the validity of the alert, and perform additional pivoting of the event to additional monitored sources in order to determine the extent of the potential threat in your environment, answering these questions:

- Is the alert that triggered just one indication of a potentially larger incident?
- Is there evidence that additional systems may be impacted?
- Can the root cause of the activity be identified?

Providing Security Analysts with a single view over the entire monitored client estate and the ability to perform threat hunting activities across these in a responsive manner, offers insight into the entire security incident life cycle.

A view enabled by supporting tools, contextual data and insights to customers sources result in the Security Analyst’s ability to offer accurate, relevant and actionable Security Incident reports.
### 2.7.2 Analyst Workbench

The Threat Detection Service enables incident investigations with a proprietary security analysis toolset called Analyst Workbench. This toolset consists of two components – ‘Inspector’ and ‘Meta’ that offer a single interface for analyst’s investigating incidents. Toolsets allows for Security Analysts to seamlessly access all monitored sources and contextual information regardless of client, source, or origin. They provide a complete picture of the identified suspicious behaviour.

**Figure 5 – Analyst Workbench**

<table>
<thead>
<tr>
<th>Inspector</th>
<th>Meta</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Manipulation – grouping, sorting</td>
<td>Signature information – Signature description, trigger information (such as Reputation, Pattern, Anomaly summary)</td>
</tr>
<tr>
<td>Context – previous escalations, IP information (Geo IP, Whois, ISP), confidence scoring</td>
<td>Enrichment – CVE information, GeoIP, Impact estimation</td>
</tr>
<tr>
<td>Temporary Monitoring – monitor a specific IOC or combination of IOCs over time for additional activity</td>
<td>Evidence data – Such as PCAP data, Sandbox trace, Endpoint data in relation to collected events</td>
</tr>
</tbody>
</table>
**Inspector**

Temporary Suppression Filters – suppress a specific IOC or combination of IOCs over time for additional activity

---

**Meta**

Threat Hunting capabilities throughout the entire client estate (e.g. Cross log-type category correlation).
Display contextual information and Evidence data in relation to events – Event, Description, PCAP, Sandbox report, CVE, Signature pattern, Endpoint reports (triage files).
Historic activities – Fetch all historic activities in relation to specific IOC’s and context in relation to these (e.g. PCAP).
Query internal and external services – The ability to instantly query multiple Threat Intelligence and Antivirus sources for additional information on potential threats and typical threat coverage.

*Table 4 – Analyst Workbench Components*

### 2.8. Automated Security Incident reports

As security incidents are identified the Security Analyst will provide you with a Security Incident report that includes a detailed description of the threat, identified activity, impact, and a recommendation of suitable incident response steps to take.

Typical content includes:

- Estimated Severity
- Activity Summary
- Incident Description
- Incident Response Recommendations

The contents of this report will significantly increase your ability to take swift and informed steps in resolution of escalated security incidents.

Given the impacts associated with security incidents are closely tied to the period of time an attacker has until detection and containment, receiving an actionable incident report significantly lowers your risks.

### 2.8.1 Security Incident Categorization

Automated security incidents are categorized below:

<table>
<thead>
<tr>
<th>Inspector</th>
<th>Meta</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access</td>
<td>Data exfiltration</td>
</tr>
<tr>
<td></td>
<td>Vulnerability exploration</td>
</tr>
<tr>
<td></td>
<td>Cross site scripting</td>
</tr>
<tr>
<td></td>
<td>SQL injection</td>
</tr>
<tr>
<td></td>
<td>Host compromised</td>
</tr>
</tbody>
</table>
## Inspector Meta

<table>
<thead>
<tr>
<th>Inspector</th>
<th>Meta</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Evidence tampering</td>
</tr>
<tr>
<td></td>
<td>Privilege escalation</td>
</tr>
<tr>
<td></td>
<td>Brute force attacks</td>
</tr>
<tr>
<td>Denial of service</td>
<td>Application DoS</td>
</tr>
<tr>
<td></td>
<td>Volumetric DDoS</td>
</tr>
<tr>
<td></td>
<td>Application DDoS</td>
</tr>
<tr>
<td></td>
<td>Latency measurement</td>
</tr>
<tr>
<td></td>
<td>Bandwidth measurement</td>
</tr>
<tr>
<td>Malicious software</td>
<td>Malware Infection</td>
</tr>
<tr>
<td></td>
<td>Exploitation attempt</td>
</tr>
<tr>
<td></td>
<td>Adware, or grayware</td>
</tr>
<tr>
<td>Improper usage</td>
<td>Instant messaging</td>
</tr>
<tr>
<td></td>
<td>Data leakage</td>
</tr>
<tr>
<td></td>
<td>Peer-to-peer activity</td>
</tr>
<tr>
<td></td>
<td>Policy violation</td>
</tr>
<tr>
<td>Reconnaissance activity</td>
<td>Network sweep</td>
</tr>
<tr>
<td></td>
<td>Host port scan</td>
</tr>
<tr>
<td></td>
<td>Network port scans</td>
</tr>
<tr>
<td>Other</td>
<td>Phishing</td>
</tr>
<tr>
<td></td>
<td>Account fraud</td>
</tr>
<tr>
<td></td>
<td>Social Engineering</td>
</tr>
<tr>
<td>Anomalies</td>
<td>Network Anomaly</td>
</tr>
<tr>
<td></td>
<td>Host Anomaly</td>
</tr>
<tr>
<td></td>
<td>Application Anomaly</td>
</tr>
</tbody>
</table>

Table 5 – Security Incident Categories
2.8.2 Example Incident Report

Example Automated Incident report with generic recommendations provided:

Security Incident Report

Customer

Device

-RTENGINE-A

Reference #

201629

Severity

Critical

Date and Time

Start Date 2016-07-11 13:10:14 (UTC)  End Date 2016-07-11 13:11:13 (UTC)

Description

The host 10.7.11.01 has triggered the signature "BOOST-O-PCH-000: Malicious behavior threshold exceeded (Internal Source IP)". This signature identifies when a single source IP-address is involved in various activity which on its own may not be suspicious, but combined highlights related activities of interest. BOOST is a correlation scoring method whereby each alert in the engine is assigned a unique score. The correlation method then maintains a sliding window of the accumulated sum of these scores, and identifies when a single source host exceeds a BOOST threshold. An overview of the activity noted by the source is listed in the following table:

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Source IP</th>
<th>Signature</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.01</td>
<td>PROXY-O.PCK-234: Suspicious rare site transitions (initial communication)</td>
<td>90</td>
</tr>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.01</td>
<td>PROXY-O.PCK-234: Suspicious file download from rare TLD</td>
<td>80</td>
</tr>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.01</td>
<td>PROXY-O.PCK-234: Suspicious file download from rare TLD</td>
<td>70</td>
</tr>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.01</td>
<td>PROXY-O.PCK-234: Suspicious file download from rare TLD</td>
<td>60</td>
</tr>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.01</td>
<td>PROXY-O.PCK-234: Suspicious file download from rare TLD</td>
<td>50</td>
</tr>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.01</td>
<td>PROXY-O.PCK-234: Suspicious file download from rare TLD</td>
<td>40</td>
</tr>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.01</td>
<td>PROXY-O.PCK-234: Suspicious file download from rare TLD</td>
<td>30</td>
</tr>
</tbody>
</table>

Summary: A total of 9 alert(s) in ~ 56 second(s)

Event extracts for the 9 alerts are detailed below:

PROXY-O.PCK-234: Suspicious rare site transitions (initial communication)

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Source IP</th>
<th>Target</th>
<th>Original Domain Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.01</td>
<td>VIP</td>
<td><a href="http://tryformypip:79/?leon=60f1faa9-44101040d19390005r=120550axr=1v">http://tryformypip:79/?leon=60f1faa9-44101040d19390005r=120550axr=1v</a> ...</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.01</td>
<td>ODV</td>
<td><a href="http://6f002b66e204abowforad.on">http://6f002b66e204abowforad.on</a></td>
<td>ACCEPT</td>
</tr>
</tbody>
</table>

PROXY-O.PCK-130: Multiple content type communication towards rare TLDs

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Source IP</th>
<th>Content Type</th>
<th>URL Host</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.01</td>
<td>text/html</td>
<td>tryformypip</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.01</td>
<td>application/x-vnd-chrome</td>
<td>6f002b66e204abowforad.on</td>
<td>ACCEPT</td>
</tr>
</tbody>
</table>
2.9. **Security Incident Reports Based on Detailed Investigation and Threat Hunting**

As security incidents are identified the Security Analyst provides you with a Security Incident report that includes a detailed description of the threat, identified activity, and impact, combined with a recommendation of suitable incident response steps to take. Typical content includes:

- Estimated Threat Severity
- Activity Summary
- Incident Description
- Incident Response Recommendations

The contents of this report will significantly increase your ability to take swift and informed steps in resolution of escalated security incidents.

Ongoing security incidents will be kept open until confirmation and validation of containment occurs. Updates may be provided as new information is identified in relation to open security incidents.

Validated security incidents are classified with appropriate threat severity based on the SOC team’s analysis and assessment.
2.10. **Client Access to 90 days of Event and Historical Incident Data**

The NTT Managed Centre portal (see section Error! Reference source not found.) allows you to review incident data over a variety of predefined timeframes.

2.11. **Client Enriched and Aggregated Log Search (Option)**

The Investigator Tool ('Investigator') provides cloud-based, real-time access to log data. Accessible through the Security portal, Investigator is available as a service option for the Threat Detection Service.

As we collect and analyse logs, it also archives a copy of logs in a secure, cloud-based repository. Online access to enriched and aggregated logs through the Security portal is enabled without the need for additional on-premises equipment or an up-front capital investment. This accessibility enables data mining of the logs for efficient security and compliance of incident investigations.

Search results can be filtered and mass exported for further off-line analysis.

*Figure 7 – Investigator*

Incident investigations require fast, efficient access to needed log data. Too often, this involves manually pulling logs from multiple sources. This process can waste precious time and may involve understanding and accessing multiple interfaces to access required log data.
Investigator provides a single source to access logs allowing the Security team to immediately investigate incidents instead of spending time locating and accessing necessary logs.

Investigator is built on a big data infrastructure, including Hadoop™ for storing large data sets, MapR™ for efficient queries, Elasticsearch® for indexing and Apache Lucene™ for simple and complex searches. These components allow for fast, flexible searches, delivering query results in seconds. Users can create queries using Boolean and wildcard searches.

When a deep dive is necessary, Investigator allows users to search for logs. Searches use standardized query language or the wizard-like filtering tool can be used to narrow specific data points. Recent searches can easily be re-run and frequent searches can be saved by each user.

Figure 8 – Investigator Log Searches

Figure 9 – Investigator Search Filtering
2.11.1 Secure Long-Term Log Storage and Management (Option)

Secure Long-term Log Storage Option is available for TD-S and TD-E clients. Secure Long-Term Log Storage utilizes the MSS infrastructure to store and retrieve raw logs collected by the platform. SLTLS will store logs for all devices in scope for Client subscribed monitoring service. SLTLS is not customizable to specific devices or IP addresses.

SLTLS utilizes the NTTSA appliance to collect logs. Client must either have a physical or virtual appliance deployed to enable SLTLS services. The SLTLS service utilizes proprietary data storage software to securely store raw logs in originally obtained unaltered format. The SLTLS solution provides data encryption at rest to ensure the privacy of Client stored logs. The data encryption at rest feature is a FIPS 140-2 Level 2 validated enterprise-class encryption solution that complies with regulations for sensitive data, such as HIPAA and Sarbanes-Oxley.

A user interface is provided so that Clients can perform raw log searches. The user interface is located within the Security Portal. Clients may specify a date range along with an IP address as required input for log searches. Results from searches are displayed in the Security Portal as a list of hourly compressed files that can be downloaded.

Log retention can be purchased in increments of 3 months (e.g. 3, 6, 9, 12, 15, 18, etc). Once the retention period has expired, raw logs shall be purged. SLTLS provides Clients the ability to self-service search for raw logs via the Security Portal. As this is a self-service offering Client is responsible for performing searches and downloading relevant log files.

Service option is not available for Clients delivered via On-premises POD infrastructure as described in section ‘2.11.2 On-premises POD.’

2.11.2 On-premises POD (Option)

TD-E Clients have the option to purchase an On-premises POD for scenarios where logs are required, or preferred to remain on-site.

2.11.3 Vulnerability Correlation (Option)

TD-E Clients subscribed to the Vulnerability Management service may benefit from added Vulnerability Correlation capabilities on an opt-in basis. Feature opt-in request are made during Client Service Transition, or raised by the Client on the Security Portal during continuous service delivery.

Upon opt-in, the Vulnerability Management service provides TD-E with added contextual information of Client assets and Vulnerabilities which are then used by
Vulnerability Correlation to increase TD-E’s overall ability to understand the relevance of a threat and raise the accuracy of Security Incident reports.

Service option prerequisites:
- TD-E Client is also subscribed to Vulnerability Management services delivered by NTT using Qualys.
- Client Qualys subscription includes access to the Qualys API and the API key is provided to NTT for integration purposes.
- Client Qualys API subscription is appropriately sized and reflect the size of the organization and its asset estate, smaller subscriptions may result in limited usages caused by Qualys API restrictions.

2.11.4 Proactive Response (Option)

TD-E Clients have the option to purchase Proactive Response capabilities. With the Proactive Response add-on option NTT shall take actions to contain/disrupt threats described in security incidents, when the Security Analyst deem it appropriate. Actions are performed on Client network devices, typically hindering, or limiting the progress of identified attacks sufficiently to provide the Client with additional time to take informed Incident Response actions.

Threat containment

In response to Security Incidents identified by the TD-E service, NTT shall take appropriate actions to block threats from traversing Client network devices. Blocking actions are implemented using Indicators of Compromises (IOCs) seen in association of threats.

Client acceptance
- Client accepts that Proactive Response actions are of Emergency Change nature and are considered outside traditional change management processes in priority of disrupting/containing threats.
- Client understands and accepts the risks associated with responsive actions and the potential negative impact it may have on the availability of the Client environment.
- NTT shall not be held liable for any negative impact’s responsive actions within the scope of Proactive Response service options may have.

Service option prerequisites
- Client Network Devices are configured in accordance with the Security Configuration Guide.
- Network design and Client’s security policy shall be configured in a manner which supports the containment actions provided by NTT.
- Client Network Devices are provided with access to the Security Incident Response Platform using Internet connectivity.
2.12. **Security Appliance**

NTT’s Managed Security Services require a Security Appliance.

The Security Appliance is available in multiple form factors, including a virtual image and physical appliance. You must install, initially configure and enrol Security Appliances. We will only be responsible for management and maintenance of the appliance software (in both physical and virtual form factors) and the physical appliance form factor if supplied by us.

Security Appliances gather logs, events, reports, and evidence data from your in-scope devices and systems, then prepare the data for secure transmission and processing. Ongoing configuration and maintenance of the Security Appliance is conducted by us. Therefore, the Security Appliance should be installed by you in a suitable location on your network infrastructure to facilitate both access and log collection.

Key features of the Security Appliance include:

- Physical or Virtual (VMWare) form factors.
- The Security Appliances run a hardened Linux operating system, fully maintained by us.
- Log and data capture with compression and secure forwarding to the NTT Data center.
- Encrypted connections to and from the NTT data center (zero touch ‘phone home’ VPN).
- Custom developed networking to address multi-tenant address space issues.
- Log storage capabilities in the event of connectivity loss.
- Provides backup of your devices under management.
- Health and availability monitoring of your devices under management.
- Multiple containerized services.
- Regional centralized control and configuration.
- In the field full OS and container upgrade capabilities.

<table>
<thead>
<tr>
<th><strong>CPU</strong></th>
<th>1 vCPU @ 4 Cores 64-bit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disk</strong></td>
<td>60 GBytes (Operating System) + 250GBytes (Data)</td>
</tr>
<tr>
<td><strong>RAM</strong></td>
<td>16 Gbytes</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>1 Network Interface</td>
</tr>
</tbody>
</table>

*Table 6 – Minimum Virtual Appliance Recommended Specifications*
2.12.1 Data Collection

Data collection is equally applicable to both Threat Detection Services and Enterprise Security Monitoring (ESM) Services for syslog sources. Added configuration is required to establish evidence collection as described in the respective technology Configuration Guides.

The first step in MSS processing is data collection. Our client installations utilize a Security Appliance to collect logs from monitored devices, then transmit logs to NTT data centers for analysis.

2.12.2 Log Transport Agents

A Log Transport Agent (LTA) is a mechanism residing on a client’s system used to transmit logs to a Security Appliance. LTAs typically consist of configuration settings for the system, however, there are occasions when additional software or agents must be installed to assist in the log transport process. We support many different types of LTAs for industry-leading security devices and applications, as well as many less common devices and applications.

We have developed multiple methods to receive log and event information. The most common method of event collection is syslog. The service can also support many less common types of log collection: SNMP traps, downloading log files through FTP, disk shares, or even interactive SSH sessions.

If you have a technology for which we do not have an existing LTA, the NTT on-staff development team and Information Security Engineers (ISEs) can develop a new LTA solution for an additional fee.

2.12.3 Configuration Guides

We will work with your technical staff to recommend and validate appropriate audit settings for each system monitored and to ensure services meet your security and compliance requirements.

To assist with this process, we have developed audit Configuration Guides for over 100 commonly monitored products. Configuration Guides for supported devices serve the following key purposes:

- **Ensure appropriate logging configuration.** Configuration guides have been developed to ensure that appropriate security logs are generated by the system being monitored.

- **Ensure Appropriate Log Transport Agent and Evidence Collection Configuration.** Configuration Guides also identify the configuration necessary for logs to be transported, properly formatted and transmitted to the Security Appliance.
3. Our Approach to Service Operations

3.1. Service Experience

Our desire is to maximize the value you receive from Managed Security Services through effective engagement, communication and information sharing. Our focus is to enhance your service experience and provide your organisation with insight to enable your business decisions.

3.2. Service Desk

NTT’s regional Managed Service Centre (MSC) is your primary Service interface, available to you 24/7/365. The NTT MSC coordinates incidents, and service requests, as well as system administration functions.

The service desk logs, tracks, and closes all tickets (incidents and service requests) in the NTT service management system. Tickets can be logged through the following methods:

- event driven (through monitoring of the environment)
- directly reported to us by you through the service desk
- directly reported to us by you via the Manage Centre portal
- directly reported by SOC via our Integrated Service Desk

3.2.1 Manage Centre Portal

As part of any Managed Security Service, you are provided with access to NTT’s Manage Centre portal. Manage Centre provides online access to:

- interact with us online by logging incidents, requests and changes
- track, view and submit comments within incident, request, and change tickets
- view contract data
- browse and search our knowledge base, and
- access the online document repository for contractual documentation, procedural documentation, meeting minutes, etc.
3.2.2 Online Dashboards and Charts

Reporting is provided via NTT’s Manage Centre portal, through a mixture of interactive dashboards, charts and downloadable reports. Through Manage Centre, users can do the following:

- View summaries and drill down into the detail for analysis.
- Focus in on specific time periods.
- Export the underlying data for offline analysis or reformatting.

1 The Managed Centre Portal provides a consolidated view of all your NTT managed services some functionality such availability, capacity and performance data do not apply to security services.
Interactive reporting is available for:

- service levels, and
- task-related data e.g. incidents, requests, changes.
4. **Service Management**

4.1. **Service Level Management**

Depending on the complexity and/or size of your environment, and the mix of products and services, we may recommend additional Service Delivery Management options.

4.1.1 **NTT Service Delivery Manager (SDM)**

Service Delivery Management provides governance and control across the various service features, processes, and systems necessary to manage the full lifecycle of the Threat Detection Services.

We will assign a Service Delivery Manager (SDM) to be responsible for service level management, and to act as an advocate for your organization within NTT. The NTT SDM is the primary interface who will manage the Service Delivery relationship between your organization and NTT. The SDM is responsible for scheduling, running all service management review meetings, and ensuring all processes and documentation are in place to manage your services.

Deliverables of the NTT SDM include:
- establish client relationship
- capture and manage minutes, agenda items, actions, and decisions
- change management issue management
- escalation management
- risk management
- service level monitoring, reporting and management
- service review meeting
- work with Service Transition Teams

4.1.2 **Technical Account Manager (TAM) (Option)**

The Technical Account Manager (TAM) is an optional resource that provides overall account management and specialized technical support to you by responding to action items, emails, and customer calls, and by proactively initiating actions to ensure client satisfaction. The TAM is the point of contact for incidents and service requests that are outside the scope of support provided by the Support Operations Center (SOC). The TAM also manages designated accounts both by responding to technical questions, issues, and opportunities; as well as by overall management of requests and general account satisfaction levels. This position is primarily technical in nature, with a high level of client interface, and requires strong prioritization and project skills.
4.2. Change management support

We will partner with your Change Advisory Board (CAB) to support changes to your environment. Standard change requests can be made via the Manage Centre portal, or a service request logged to the NTT MSC. More specifically, you can request Moves, Adds, Changes, Deletions (MACDs) to your configuration items and for minor configuration changes that have been pre-approved by your CAB as standard changes.

4.2.1 Change request management

We will manage Requests for Changes (RFCs) on your behalf through the change lifecycle, including:

- providing a method for logging RFCs
- classifying and managing a change in accordance with its classification:
  - standard (pre-approved) changes
  - normal changes
  - urgent changes
  - emergency changes
- requesting an impact analysis to be completed by the appropriate client stakeholders
- distributing relevant documentation for review prior to CAB meetings
5. **Our Approach to Service Transition**

Our approach to transition aims to ensure that both organizations enter the transition with a clear idea and understanding of the goals and objectives of the transition.

5.1. **Objectives of Service Transition**

- To ensure the absolute minimal business disruption during the transition of the managed service.
- To facilitate a smooth and trouble-free transition.
- To determine and manage realistic transition timeframes.
- To establish an operational baseline for the global managed services delivery organization that will be responsible for delivering the service post-transition.
- To facilitate and conclude the contracting process.
- To develop and build a sound business relationship from the onset.
- To align your expectations with service delivery capabilities and constraints.
- To ensure our people understand your business from the onset to deliver a reliable, stable and excellent service.

5.2. **Transition Methodology**

We use a formal transition methodology, developed in-house from industry-leading best practices and years of practical experience with the transition of operations from its clients and/or incumbent service providers. It is a formal methodology that allows flexibility for adjustment to cater for a wide spectrum of operational services, assets, staff, policies, process, standards and architectures to be transferred to us.

NTT's Service Transition Manager is responsible for managing the transition process with you and your organization and coordinating back with our Centre of Excellence (COE) Transition Team. The COE Transition Team is responsible for running the service activation process to enable service operations. As part of the service activation process, the tools and systems are setup and activated for the managed service to go live.

The typical duration for service transition is 12 weeks, although timing will depend on the size and complexity of the environment.

5.2.1 **Managed Devices**

Managed Devices must be Healthy, Functional and Tuned before we will accept the management responsibility during the Go LIVE phase.

‘Healthy’ means there are no known hardware/software issues or bugs affecting the operation or management of the configuration item.
‘Functional’ means the configuration item has been specified and designed correctly, has been configured and is operationally effective.

‘Tuned’ means the configuration item has been configured according to the needs and relevance of your environment, including minimizing false positive alerts and ensuring redundant or unnecessary configurations are removed.
## Appendix A  Service Level Agreements

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Priority</th>
<th>SLA</th>
<th>Service Credits</th>
<th>Service Credit Limit</th>
<th>Service Calendar</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Availability - Client Portal</strong></td>
<td>The Client Portal is available 24 hours a day, 365 days a year with a 99.8% up-time guarantee (not including scheduled maintenance windows).</td>
<td>N/A</td>
<td>99.5%</td>
<td>5% of Monthly Service Fee</td>
<td>25% of Monthly Service Fee</td>
<td>24x7</td>
</tr>
<tr>
<td><strong>Emergency Request assignment response</strong></td>
<td>NTT will assign a Service Request ticket within 30 minutes from the client assigning the Service Request ticket to the NTT Service Desk.</td>
<td>N/A</td>
<td>30 mins</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Standard change/Normal Request assignment response</strong></td>
<td>NTT will assign a Service Request ticket within 30 minutes from the client assigning the Service Request ticket to the NTT Service Desk.</td>
<td>N/A</td>
<td>60 mins</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Request Complete - Emergency request (RFC)</strong></td>
<td></td>
<td>P1</td>
<td>2 Business days</td>
<td>100% Service Units of the Request</td>
<td>100% Service Units of the Request</td>
<td>24/7</td>
</tr>
<tr>
<td><strong>Request Complete - Request for information / Standard change</strong></td>
<td></td>
<td>P1</td>
<td>2 Business days</td>
<td>100% Service Units of the Request</td>
<td>100% Service Units of the Request</td>
<td>24/7</td>
</tr>
</tbody>
</table>