Client Service Description

Enterprise Security Monitoring Service
Client Service Description
Enterprise Security Monitoring 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shall be binding on the parties for a period of five (5) years from the issue date stated on the front cover unless superseded by confidentiality provisions detailed in a subsequent agreement.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

Enterprise Security Monitoring Service

{Subject}

Document Preparation

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepared:</td>
<td>Jason Breytenbach</td>
<td>20 Sep 2018</td>
</tr>
<tr>
<td>Updated</td>
<td>Mike Oberholtzer</td>
<td>01 Feb 2019</td>
</tr>
<tr>
<td>Updated</td>
<td>Bob Gordon</td>
<td>05 Jun 2019</td>
</tr>
<tr>
<td>Updated</td>
<td>Sharon Witheriff</td>
<td>06 Jun 2019</td>
</tr>
<tr>
<td>Updated</td>
<td>Bob Gordon</td>
<td>02 Aug 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></td>
<td>Internal DRAFT</td>
</tr>
<tr>
<td>1.4</td>
<td>06 Jun 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** .................................................................. 7  
   1.3. **Supported Device List** ........................................................ 9  
   1.4. **NTT’s Managed Security Services Portfolio** ....................... 9  

2. **Detailed Service Element Descriptions** .............................. 11  
   2.1. 24/7 Security Operations Center Coverage .......................... 11  
   2.2. Global Threat Intelligence Center ....................................... 11  
   2.3. Standardized Event Detection and Compliance Profile .......... 12  
   2.4. Customized Event Detection and Compliance Profile for Large Range of Devices ................................................................. 13  
   2.5. Automated Analysis with Security Analyst Verification ......... 13  
   2.6. Analyst Created Security Incident Reports ........................... 13  
   2.7. Customizable monitoring and compliance reporting .......... 13  
   2.8. Access to 90 Days of Event and Historical Incident Data ........ 17  
   2.9. Client Enriched and Aggregated Log Search (Option) .......... 17  
   2.10. Secure Long-Term Log Storage and Management (Option) ... 19  
   2.11. **NTT Security Appliance** .................................................. 20  

3. **Our Approach to Service Operations** .................................. 23  
   3.1. **Service Experience** .............................................................. 23  
   3.2. **Service Desk** ...................................................................... 23  

4. **Service Management** ................................................................. 26  
   4.1. **Service Level Management** ............................................... 26  
   4.2. Change management support ................................................ 26  

5. **Our Approach to Service Transition** .................................... 28  
   5.1. **Objectives of Service Transition** ....................................... 28  
   5.2. **Transition Methodology** ..................................................... 28  

Appendix A **Service Level Agreements** .................................... 30
Client Service Description
Enterprise Security Monitoring Service

{Subject}

List of Figures
Figure 1 – Global Managed Security Service Platform ................................................................. 9
Figure 2 – Global Delivery Model .................................................................................................. 11
Figure 3 – Enterprise Security Monitoring Sample of Automated Incident Report ................. 17
Figure 4 – Investigator .................................................................................................................... 18
Figure 5 – Investigator Log Searches .............................................................................................. 19
Figure 6 – Investigator Search Filtering ......................................................................................... 19

List of Tables
Table 1 – Service Matrix .................................................................................................................. 9
Table 2 – Supported Device Vendor Table ....................................................................................... 9
Table 3 – Automated Security Incidents ......................................................................................... 15
Table 4 – Minimum Virtual Appliance Recommended Specifications ........................................... 21
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.

**Enterprise Security Monitoring (ESM)** utilizes the Global Managed Security Services Platform to provide enterprise security detection and compliance monitoring. Two types of security monitoring services are available from NTT Security: Standard and Enhanced. Both ESM Service Packages use customized rules and anomaly-based security detection and compliance profiles to identify and report on the following categories of Security events.

- **Compliance** – Events that indicate a deviation from a pre-defined baseline of a regulatory body’s definition of compliance controls.
- **Security Best Practices** – Events that indicate a deviation from pre-defined baseline of NTT Security’s definition of security best practices.
- **Business Policy Compliance** – Events that indicate a deviation from pre-defined baseline of an organisation’s custom business policy compliance requirements.
- **Enterprise Security Monitoring Standard (ESM-S)** – Standard services have been designed for organizations with standardized security detection and compliance requirements across a core set of security technologies.
- **Enterprise Security Monitoring Enhanced (ESM-E)** – Enhanced services have been designed for organizations with custom security detection and compliance requirements across a wide set of security technologies (ESM-E includes support for almost 200 different technologies).
Client Service Description
Enterprise Security Monitoring Service

The Service provides:
- 24/7 Security Operations Center coverage.
- Client notifications.
- Analyst created security incident reports.
- Automated analysis with Security Analyst verification.
- Customizable web portal.
- Client access to 90 days of Event and Incident data.

The benefits include:
- Safeguard your business by gaining 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. With Managed Device Response, threat exposures can be minimized or contained.
- 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 Analysts using advanced SOC toolsets.
- Improved agility by freeing up your internal resources to focus on your core business outcomes and requirements.
- Access to Security Operations Center (SOC) for 24/7 support and escalated engineering.

1.2. Service Matrix

The Enterprise Security Monitoring 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.
## Client Service Description

**Enterprise Security Monitoring Service**

### Service Elements

<table>
<thead>
<tr>
<th>Service Elements</th>
<th>Monitoring Services</th>
</tr>
</thead>
</table>

### Core Service Elements

- **24/7 Hours of Operation**  
  - ✔  
  - ✔

- **Security Operations Centers**  
  - ✔  
  - ✔

### Service Transition

- **Client Transition**  
  - ✔  
  - ✔

### Detection Types

- **Security Best Practices and basic compliance profile**  
  - ✔  
  - ✔

- **Enhanced compliance profile (PCI, HIPAA)**  
  - ✔

- **Customized Event detection**  
  - ✔

### Security Analyst Interaction

- **Automated Event analysis**  
  - ✔  
  - ✔

- **Custom Event analysis with Security Analyst Verification**  
  - ✔

- **24/7 Security Analyst assistance**  
  - ✔

### Client Notification

- **Automated email notifications**  
  - ✔  
  - ✔

- **24/7 Security Analyst telephone notifications**  
  - ✔

### Service Portal and Reporting

- **Service portal**  
  - ✔  
  - ✔

- **Configurable reporting**  
  - ✔  
  - ✔

- **Client access to 90 days of Event and Security Incident data**  
  - ✔  
  - ✔

### Service Options

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

- **[Option] Secure Long-term Log Storage and Management**  
  - ✔
Table 1 – Service Matrix

1.3. **Supported Device List**

Supported devices by vendor for the Enterprise Security Monitoring Services are presented in the following table:

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Amazon Web Services</th>
<th>Apache</th>
<th>Aruba</th>
</tr>
</thead>
<tbody>
<tr>
<td>3Com</td>
<td>Brocade</td>
<td>Carbon Black</td>
<td>Checkpoint</td>
</tr>
<tr>
<td>Barracuda</td>
<td>CyberArk</td>
<td>Cylance</td>
<td>Dell</td>
</tr>
<tr>
<td>Cisco</td>
<td>F5 Networks</td>
<td>FireEye</td>
<td>Forcepoint</td>
</tr>
<tr>
<td>Eclipse</td>
<td>HP</td>
<td>IBM</td>
<td>Imperva</td>
</tr>
<tr>
<td>Fortinet</td>
<td>Juniper</td>
<td>Microsoft</td>
<td>McAfee</td>
</tr>
<tr>
<td>Infoblox</td>
<td>Oracle</td>
<td>Palo Alto</td>
<td>Pulse Secure</td>
</tr>
<tr>
<td>Nortel</td>
<td>Sonicwall</td>
<td>Sophos</td>
<td>Squid</td>
</tr>
<tr>
<td>RSA</td>
<td>Thinkst</td>
<td>Trend Micro</td>
<td>Tripwire</td>
</tr>
<tr>
<td>Unix/Linux</td>
<td>VMware</td>
<td></td>
<td>Zscaler</td>
</tr>
</tbody>
</table>

Table 2 – Supported Device Vendor Table

Note. Device support varies between the Standard and Enhanced Service Packages. Please contact your NTT Sales Executive for the current list of supported devices and which Service Packages they are supported under.

1.4. **NTT’s Managed Security Services Portfolio**

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

![Global Managed Security Service Platform](image)
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.

- **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.** The Vulnerability Management Services deliver 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 Enterprise Security Monitoring service is delivered out of multiple Security Operations Centers (SOC) 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.

![Figure 2 – Global Delivery Model](image)

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 our clients’ networks. 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. **Standardized Event Detection and Compliance Profile**

NTT’s Enterprise Security Monitoring – Standard (ESM-S) Service utilizes the Global Managed Security Services Platform to provide enterprise security compliance monitoring. The level of compliance has been designed for organisations with standardized security detection and compliance requirements across a core set of security technologies.

The following sections discuss the features of the NTT ESM-S service.

2.3.1 **Detection Type**

The ESM-S service uses a standardized rule and anomaly-based security and compliance profile. NTT’s Standard Rule sets for existing supported device types are included in the ESM-S service. To ensure service quality, we will continuously make detection tuning decisions based on the validity and relevance of service generated Events and Security Incidents.

2.3.2 **Client Notification**

Automated Security Incident reports are utilized for the ESM-S service. You are notified based on your selection of NTT supported notification options, including e-mail and phone calls.
2.4. **Customized Event Detection and Compliance Profile for Large Range of Devices**

The Enterprise Security Monitoring – Enhanced (ESM-E) Service has been designed for organizations with custom security detection and compliance requirements across a wide set of security technologies (ESM-E includes support for almost 200 different technologies).

The following sections discuss the features of the NTT’s ESM-E service.

2.4.1 **Detection Type**

The ESM-E service uses customized rules and an anomaly-based security detection and compliance profile. To ensure service quality, we will continuously make detection tuning decisions based on the validity and relevance of service generated Events and Security Incidents.

Use of the NTT Standard Rule sets for existing supported device types is included in the ESM-E service.

Up to fifteen (15) Compound Rules can be developed and implemented annually for ESM-E service clients.

2.4.2 **Client Notification**

Security Incident Reports are created by Security Analysts in the ESM-E Service. You are notified based on your selection of NTT supported notification options, including e-mail and phone calls.

2.5. **Automated Analysis with Security Analyst Verification**

2.5.1 **Standard Service**

The ESM-E Service also utilizes automated detection for high confidence Security Incidents. With ESM-E, a Security Analyst verification is performed for Security Incidents ensuring that Security Incidents have been properly vetted prior to allocating resources for remediation.

2.6. **Analyst Created Security Incident Reports**

Use of standard Security reports is included as part of the ESM-S and ESM-E Services. Development of custom reports is not included in either Service.

2.7. **Customizable monitoring and compliance reporting**

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 Severity
- Activity Summary
- Incident Description
- Incident Response Recommendations

The contents of these recommendations will significantly increase your ability to take swift and informed steps in resolution of escalated Security Incidents. Given that the impact 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 lower your risk.

### 2.7.1 Security Incident Categorization

Automated Security Incidents may be categorized as follows:

<table>
<thead>
<tr>
<th>Category</th>
<th>Sub-Categories</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>
<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>
</tbody>
</table>
### Table 3 – Automated Security Incidents

<table>
<thead>
<tr>
<th>Category</th>
<th>Sub-Categories</th>
</tr>
</thead>
<tbody>
<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>
2.7.2 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 10.7.11.101 has triggered the signature "BOOST-O.PCX-005: 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 where 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>
</tr>
</thead>
<tbody>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.101</td>
<td>PROXY-O.PCX-234: Suspicious rare site transitions (initial communication)</td>
</tr>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.101</td>
<td>PROXY-O.PCX-234: Suspicious rare site transitions (initial communication)</td>
</tr>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.101</td>
<td>PROXY-O.PCX-234: Suspicious rare site transitions (initial communication)</td>
</tr>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.101</td>
<td>PROXY-O.PCX-234: Suspicious rare site transitions (initial communication)</td>
</tr>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.101</td>
<td>PROXY-O.PCX-234: Suspicious rare site transitions (initial communication)</td>
</tr>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.101</td>
<td>PROXY-O.PCX-234: Suspicious rare site transitions (initial communication)</td>
</tr>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.101</td>
<td>PROXY-O.PCX-234: Suspicious rare site transitions (initial communication)</td>
</tr>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.101</td>
<td>PROXY-O.PCX-234: Suspicious rare site transitions (initial communication)</td>
</tr>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.101</td>
<td>PROXY-O.PCX-234: Suspicious rare site transitions (initial communication)</td>
</tr>
</tbody>
</table>

**Summary:** A total of 9 alerts in 10 seconds.

Event extracts for the 9 alerts are detailed below:

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

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Source IP</th>
<th>Destination URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>VIP</td>
<td><a href="http://trifinity.vip/?h=6a0651fae9922459d8g1093003de0c12a052a01a43">http://trifinity.vip/?h=6a0651fae9922459d8g1093003de0c12a052a01a43</a>...</td>
</tr>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>GDN</td>
<td><a href="http://f600bz606s204.toopenad.gdn/">http://f600bz606s204.toopenad.gdn/</a></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Source IP</th>
<th>Content Type</th>
<th>URL Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.101</td>
<td>text/html</td>
<td>trifinity.vip</td>
</tr>
<tr>
<td>2016-07-11 13:10:14 (UTC)</td>
<td>10.7.11.101</td>
<td>application/x-chomium-fz</td>
<td>f600bz606s204.toopenad.gdn</td>
</tr>
</tbody>
</table>

---
2.8. Access to 90 Days of Event and Historical Incident Data

The Managed Centre portal allows you to review incident data over a variety of predefined timeframes. You can customize these reports by filtering on specific fields such as dates, locations and status, etc. The Security Incident data is presented along with incident data for other NTT services providing a single incident resource for all applicable subscriptions.

In addition, both ESM-S and ESM-E clients will have access to a customizable web portal that includes access to 90 days of Events and Security Incidents. ESM-S and ESM-E clients will also have access to monitoring and compliance reporting.

2.9. Client Enriched and Aggregated Log Search (Option)

The Investigator Tool (‘Investigator’) provides cloud-based, real-time access to log data. Investigator is available as a service option for ESM-E.

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

![Investigator](image)

**Figure 4 – Investigator**

Incident investigations require fast, efficient access to required 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 a 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 5 – Investigator Log Searches

Figure 6 – Investigator Search Filtering

2.10. Secure Long-Term Log Storage and Management (Option)

Secure Long-term Log Storage Option is available for ESM-S and ESM-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 services. 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.

2.11. **NTT 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. All Security Appliances must be installed, initially configured and enrolled by you. 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 in-scope client devices and systems, then prepare the data for secure transmission and processing. Ongoing configuration and maintenance of the Security Appliance is conducted by us and therefore the 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 NTT Security.
- Log and data capture with compression and secure forwarding to the NTT data center.
- Encrypted connections to and from 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.
Client Service Description
Enterprise Security Monitoring Service

- Provides backup of client devices under management.
- Health and Availability Monitoring of client devices under management.
- Multiple containerized services.
- Regional centralized control and configuration.
- In the field full OS and container upgrade capabilities.

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

Table 4 – Minimum Virtual Appliance Recommended Specifications

2.11.1 Data Collection

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

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

2.11.2 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.
2.11.3 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 NTT Manage Centre portal
- directly reported by Security Operations Centers 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 our 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.
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 Enterprise Security Monitoring 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 SDM is the primary interface who will manage the Service Delivery relationship between your organization and NTT. The SDM is responsible for scheduling and running all service management review meetings, and ensures all processes and documentation are in place to manage your services.

SDM deliverables 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

4.2. 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 Service Requests logged to the 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 Management – ESM-E

Use of the NTT Security Standard Rule sets for existing supported device types is included in the ESM-E service.

Up to fifteen (15) Standard or Compound Rules can be developed and implemented annually for ESM-E Service clients.

Additional Standard or Compound Rules can be purchased via the MACD process at a rate of 6 MACDs per rule.

Up to five (5) existing Analysers can be implemented annually for ESM-E Service clients.

Additional existing Analysers can be purchased via the MACD process at a rate of 12 MACD’s per Analyzer.

Development of new Analysers can be purchased via the MACD process at a rate to be determined based upon the level of effort associated with the development of the Analyzer.
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>
</tr>
</thead>
<tbody>
<tr>
<td>Availability - Client Portal</td>
<td>The NTTS 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>
</tr>
<tr>
<td>Emergency Request assignment response</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>
</tr>
<tr>
<td>Standard change/Normal Request assignment response</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>
</tr>
<tr>
<td>Request Complete - Emergency request (RFC)</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>
</tr>
<tr>
<td>Request Complete - Request for information/Standard change</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>
</tr>
</tbody>
</table>