Client Service Description

Threat Detection Services

20 October 2020 | Document Version 1.9

NTT contact details

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

FirstName LastName - {Job Title}, Mobile Phone: +1 203 446 4942

NTT Limited
☏ 000 000 00000
🖷 000 000 00000
✉ firstname.lastname@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shall be binding on the parties for a period of five (5) years from the issue date stated on the front cover unless superseded by confidentiality provisions detailed in a subsequent agreement.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

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.

Document Preparation

	Name	Title	Date
Prepared:	Paul Asdagi	Service Director – Group Security	12 Sep 2018
Prepared	Mike Oberholtzer	Sr. Product Manager	01 Feb 2019
Prepared	Bob Gordon	Portfolio Director - Security	05 Jun 2019
Updated	Sharon Witheriff	Technical Writer	07 Jun 2019
Updated	Bob Gordon	Portfolio Director – Security	02 Aug 2019
Updated	Tore Terjesen	Director	12 May 2020
Updated	Tore Terjesen	Director	06 October 2020
Updated	Tore Terjesen	Director	20 October 2020

Release

Version	Date Released	Pages	Remarks
1.3	05 Jun 2019	35	Internal Draft
1.4	05 Aug 2019	All	Added Severity & Confidence Settings Service Options: • [Option] Secure Long-Term Log Storage Management • [Option] Vulnerability Correlation • [Option] Proactive Response
1.5	19 Oct 2019	All	Rebrand
1.6	12 May 2020	All	Major update of the entire document
1.7	06 Oct 2020	All	Added Cloud support (AWS and Azure) Added End Point Support & Remote Isolation option New Security Incident Categories New Security Incident Report for TD-E Updated TD-S Incident Report
1.8	20 Oct 2020	36	Added Cyber Threat Sensor
1.9	1 Dec 2020		SLA Added

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

List of Figures

List of Tables

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, 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 NTT's Security Operation Centres (SOCs) or sent to you directly as a Security Incident Report depending on the Service variant you have subscribed to.

Threat Detection Services are available in two Service variants – Standard and Enhanced.

Threat Detection – Standard (TD-S) is an automated service with no Security Analyst investigation. If a threat is identified with a certain Confidence, it is sent directly to you from the Advanced Analytics engine 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.

Figure 1 Threat Detection Standard

Threat Detection – Enhanced (TD-E) is a service that identifies suspicious activities along with all the relevant contextual information. This is presented to a Security Analyst who engages in threat hunting and threat validation activities to verify the threat, its impact, and to identify additional information associated with the potential breach.

Figure 2 Threat Detection Enhanced

Once the activity is validated, the Security Analyst creates a detailed Security Incident Report and initiates security incident notifications according to client-specific procedures. The Security Analyst includes a detailed description of the security incident combined with scenario-specific actionable response recommendations which significantly assists in reducing the time taken for informed responsive measures, thereby lowering associated risks.

Clients subscribing to Threat Detection – Enhanced have the ability to add response options for containment of threats both on network devices and end points.

The Threat Detection Services provide:

- 24/7 Security Operations Centre coverage
- Services enhanced by the Global Threat Intelligence Centre
- Continuous Threat Intelligence updates driven by production investigations
- Advanced analytics with proprietary machine learning / behavioural modelling
- Automated Security Incident Reports (Standard only)
- Manage Centre Portal
- Vendor integration and evidence collection for key security technologies (Enhanced only)
- Event driven threat hunting (Enhanced only)
- Detailed security incident investigation by Security Analysts (Enhanced only)
- Client access to 90 days of event data
- Client access to security incidents

Key Benefits

- Better protection of information assets to minimize any impact on business operations and reduce overall security risk.
- Rapid identification, prioritization, and response to cyber-security attacks.
- 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.
- Containment and blocking of identified threats (Enhanced only).
- Certified SOC environments to protect your data: ISO/IEC 27001:2017, SOC2 Type 1, ASIO-T4 (Australia).

1.2. Service Matrix

The Threat Detection Services are available in two distinct Service variants.

The service variant, selected options and associated service levels forms part of your Managed Services Agreement.

Service Features	Service Variant	
	Standard	Enhanced
Core Service Features		
• Hours of Operation (24/7) • Security Operation Centres (SOCs) • Client Portal • Language Support • Security Appliance	✓	✓
Threat Detection Service Features		
Service Portal and Reporting		
Security Incidents	✓	✓
Manage Centre Portal	✓	✓
Client Access to 90 days of Event Data	✓	✓
Threat Intelligence		
Services Enhanced by NTT Global Threat Intelligence Centre	✓	✓
Continuous Threat Intelligence Updates Driven by Production Investigations	✓	✓
Detection Types		
Advanced Analytics with Proprietary Machine Learning / Behavioural Modelling	✓	✓
Security Analyst Interaction		
Automated analysis	✓	
Detailed Security Incident Investigation by Security Analyst		✓
Event-driven Threat Hunting		✓
Vendor Integration and Evidence Collection for Key Security Technologies[1]		✓

[1] Gathers and analyses evidence data in relation to vendor alerts, such as PCAPs and execution reports.

Service Features	Service Variant	
	Standard	Enhanced
Client Notification		
Automated Security Incident Reports	✓	
Analyst-created Security Incident Reports based on Detailed Investigation and Threat Hunting		✓
Service Options		
Cyber Threat Sensor (CTS)		✓
Investigator – Enriched and Aggregated Log Search		✓
Secure Long-Term Log Storage (SLTLS)	✓	✓
Vulnerability Correlation		✓
Proactive Response		✓
Remote Isolation		✓
Service Management		
24/7 Service Desk	✓	✓
Service Level Management	✓	✓
Service Delivery Manager	✓	✓
Technical Account Manager (option)	✓	✓
Service Transition		
Client Transition	✓	✓

Table 1 Service Matrix

1.3. Supported Device Categories

The following table lists supported devices by log source category. Support applies to HW, virtual and cloud based sources.

Firewall	Proxy/URL	IDS/IPS	Sandbox
End Point (EDR)	Antivirus	Webserver	Operating System
DNS	Email GW	Authentication	Netflow

Table 2 Threat Detection Log Source Support by Category

Note. Device support varies between the Standard and Enhanced service variants. Please contact your NTT Sales Executive for the current list of supported vendor technologies and the specific support under each service variant.

1.4. NTT's Managed Security Services Portfolio

Figure 3 MSS Service Menu

2. Core Service Feature Descriptions

2.1. Hours of Operation

Threat Detection Services are delivered through our Security Operation Centers, which operate 24 hours a day, 7 days a week.

2.2. Security Operations Centres (SOCs)

We will deliver Threat Detection Services from any of our SOCs at our sole discretion. Your data may be stored in any of the SOCs and on our global infrastructure unless there is prior agreement and approval between NTT and you.

You will be provided with the contact details of the relevant SOC during service transition.

2.3. Client Portal

You will have access to our Manage Centre Portal which is a globally available, web-based application which allows you to interact with, manage, and monitor your Managed Security Service.

2.4. Language Support

Threat Detection Services are provided in the English language only, unless there is prior agreement and approval between NTT and you.

2.5. Security Appliance

Managed Security Services (MSS) require a Security Appliance for most supported environments, technologies and sources. Certain cloud environments and sources are supported without the Security Appliance.

When cloud sources have no Security Appliance dependency, as defined by NTT, Log Transport Agents (LTAs) will be configured to gather logs, events and evidence directly from your cloud instance without flowing through your premise and removing the requirement for 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 log feeds 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 form factors
- public cloud support

- 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 NTT data center (zero touch 'phone home' VPN)
- custom developed networking to address multi-tenant address space issues
- provides secure access for backup and restore of client devices under management
- health and availability monitoring of your devices under management, and
- centralized management and configuration.

The Security Appliance requires:

- One or two static non-dynamic IP addresses (depending on the environment)
- Permanent LAN Connectivity
- Permanent Internet connectivity on TCP port 443

For the virtual form factor, the Security Appliance also requires:

- Configuration to power on automatically, if the hypervisor is restarted
- Minimum resources from the hypervisor in the virtual environment, as specified by NTT

2.5.1 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 Configuration Guides for the 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 or directly to NTT's data centre.

3. Detailed Service Feature Descriptions

3.1. Service Portal and Reporting

3.1.1 Security Incidents

The Security Incident Report is the main deliverable for Threat Detection Services. For Threat Detection - Enhanced you will receive a Security Incident Report written by a Security Analyst. If you subscribe to Threat Detection - Standard, the Service creates the report automatically.

3.1.1.1 Security Incident Definitions (Standard / Enhanced)

Severity definitions for security incidents are presented in the following table.

Severity	Definition	Applicable Services
Low	Observed security related event that could be an interesting security event, not a security incident.	TD – Standard / Enhanced
Medium	Minor security incident with low risk to spread or propagate. Should be tracked and followed up but will in general not require immediate actions.	TD – Standard / Enhanced
High	Security incident and if exploited, can lead to system compromise and/or loss of information. Should be investigated in a timely fashion.	TD – Standard / Enhanced
Critical	**Analyst-validated** security incident with severe impact and threatens to have a significant adverse impact in the affected system. These issues have high probability to spread or propagate, pose a threat to confidential or sensitive data or assets. Critical security incidents require immediate attention for remediation or mitigation.	TD – Enhanced

Table 3 Severity Definitions

These are to be considered guidance only. The Security Analyst always have final say in assigning the threat severity while considering the situation and past experiences (Threat Detection – Enhanced).

3.1.1.2 Threat Detection - Enhanced Security Incident Categorization

Validated Threat Detection - Enhanced security incidents (and events) are assigned a category from the following list which is based on MITRE ATT&CK tactics:

- Unspecified
- Initial Access
- Execution
- Persistence

- Privilege Escalation
- Defence Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration (& Destruction)
- Impact
- Technical Information Gathering (Pre-ATT&CK)
- Technical Weakness Identification (Pre-ATT&CK)

3.1.2 Manage Centre Portal

As part of any Managed Security Service from NTT, 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.

Ticket level reporting is provided via 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, and
- export the underlying data for offline analysis or reformatting.

Figure 4 Manage Centre Dashboards and Reports

3.1.3 Security Tools

For Threat Detection you are provided with a set of Manage Centre Security tools for real time investigational purposes:

- Security Event List viewer
- Security Event List dashboard

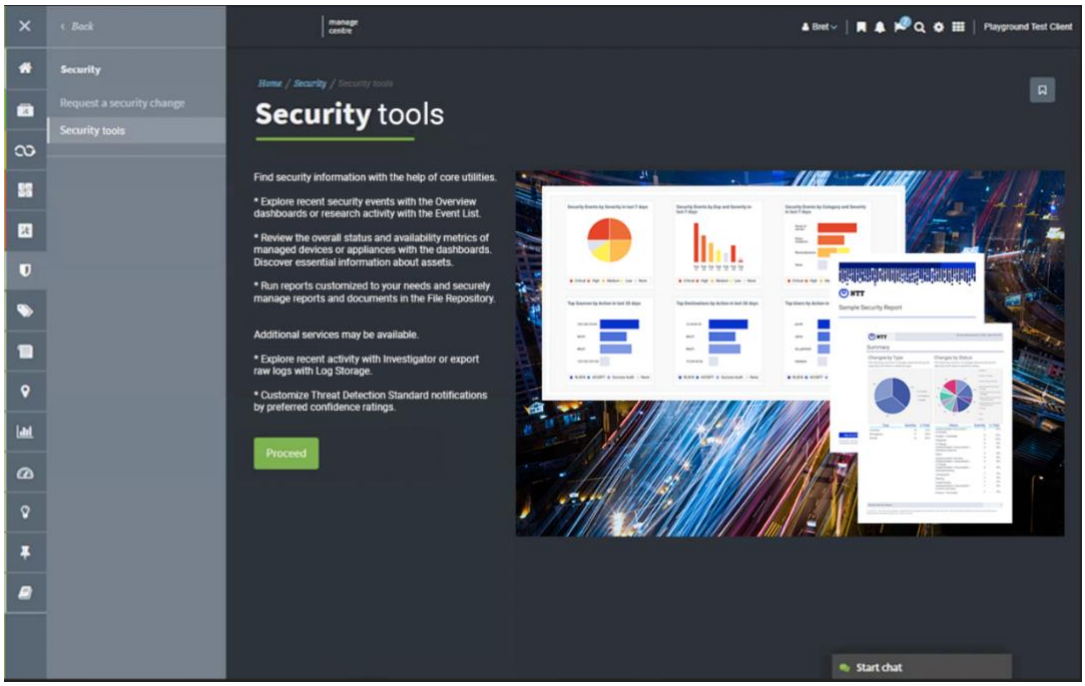


Figure 5 Manage Centre Security tools

In addition to the standard features, Security tools also include access to additional investigation and log storage options:

- Investigator, an Enriched and Aggregated Log Search tool
- Secure Long Term Log Storage (RAW log storage)

These options are described in *3.6 Service Options*.

3.1.3.1 Security Event List and Dashboard

The Security Event List tool allows you to search for security events triggered by the threat detection analysis engine and your security devices. Data is available for the last 90 days. Event list output can be exported as PDF or Excel documents.

You also have access to the Threat Detection Event Overview Dashboard that contains:

- Security Events by Severity in the Last 7 Days
- Security Events by Day and Severity in the Last 7 Days
- Security Events by Category and the Severity in the Last 7 Days
- Top Sources by Action in the Last 30 Days
- Top Destinations by Action in the last 30 Days
- Top Users by action in the Last 30 Days

3.2. Threat Intelligence

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.

3.2.1 NTT's Global Threat Intelligence Centre

Dedicated Threat Intelligence Analysts in the Global Threat Intelligence Centre 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, and
- collaboration with data scientists improve machine learning capabilities.

3.2.2 Continuous Threat Intelligence updates

Product threat data is gathered from the global network of analysis engines monitoring your 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 high confidence 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.

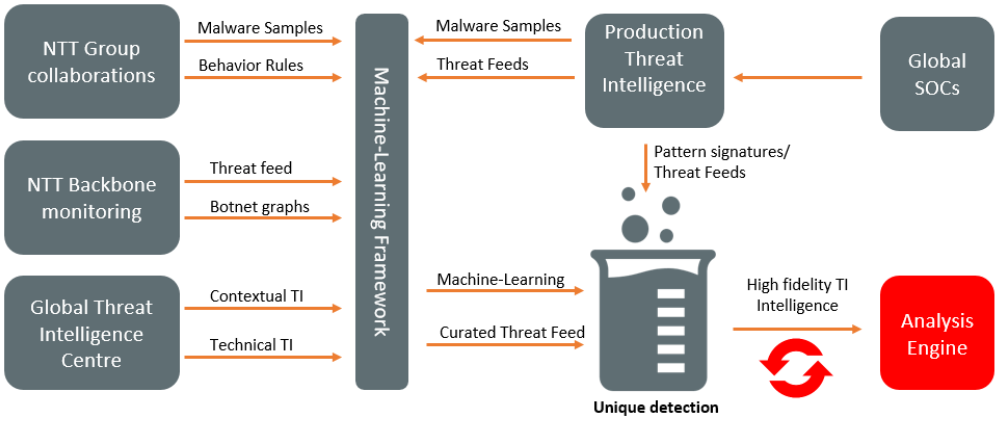


Figure 6 Continuous Threat Intelligence Updates

3.3. Detection Types

3.3.1 Advanced Analytics

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 our 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:

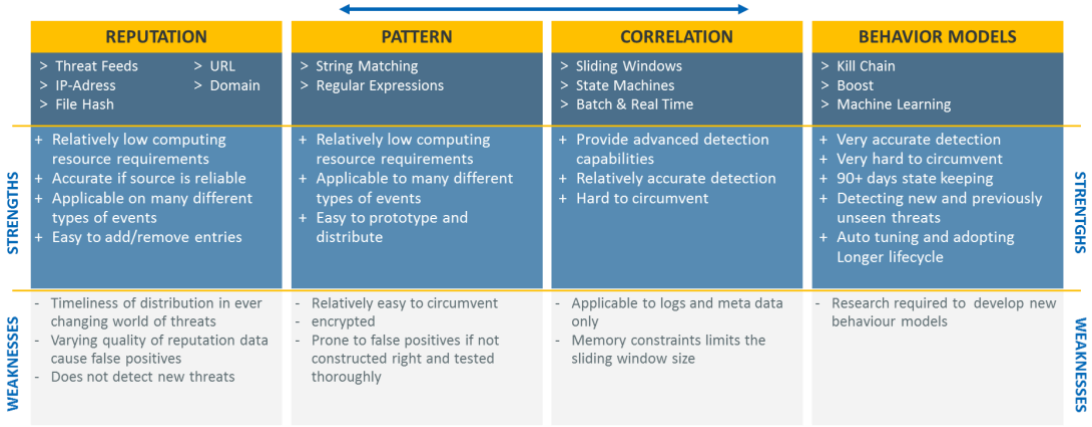


Figure 7 Detection Capabilities

Attackers use of a variety of Tools, Techniques, Procedures (TTPs) to reduce 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 coverage 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.

3.3.1.1 Machine Learning

The analysis engine used for delivery uses a set of supervised and unsupervised machine learning techniques to enable detection of evasive and previously unknown threats using anomaly identification.

As described in 3.2.2 Continuous Threat Intelligence updates, the analysis engines are frequently updated with new behavioural patterns and anomaly detection techniques that address the latest threats and potential changes in associated threat behaviour.

Usage of threat classifiers and anomaly detection enable NTT to identify previously unseen threats and threats using evasion techniques where reputation and signature-based detection provide limited value.

3.3.1.2 Threat Behaviour Modelling

Most software has a specific executional order and frequency built in – malware is no exception to this. While today's malware more frequently employs evasion techniques to avoid most detection techniques, the executional order of specific malware families is rarely masked, or undergo significant change.

Machine learning and statistical modelling capabilities are used to identify such behaviour order and frequencies to build out threat behaviour model signatures. This enable a persistent method of detecting malware based on this behaviour instead of IOC's and patterns normally used by traditional signatures and reputation techniques.

3.3.1.3 Anomaly Detection

Statistical modelling on authentication and change logs to profile activity in your cloud or traditional environments. This allows for detection of anomalies that contribute to existing threat models. These anomalies are mainly related to administrator activity (account creation, password resets, etc), focused on temporal features (weekday, time) and access patterns (IP used for login etc). An example of an established profile is shown in Figure 8 Example, Statistical modelling of Administrator activity, where an office-hour distribution can be seen over a 6-month period (excluding password resets).

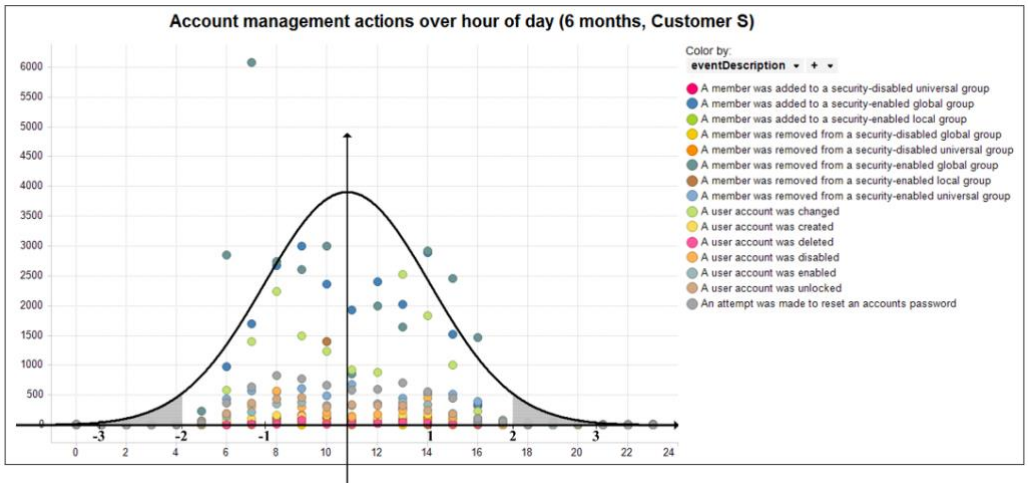


Figure 8 Example, Statistical modelling of Administrator activity

Anomalies which can be tied to a suspected compromise contribute to existing threat models. Note that these models are built over longer time periods and may need to be rebuilt if major changes are made in your environment.

3.3.1.4 Cyber Kill Chain

Originally used by military services as a method to define and categorize the phases of an attack into stages. The idea is that if one of the multiple phases of an attack are disrupted the defender has the opportunity to interrupt the kill-chain and by doing so stop the attack.

Based on this concept, Lockheed Martin introduced the Cyber Kill-Chain as a standardized means to describe the different phases of an attack life cycle for the IT security industry. Reusing the same concept, disrupting one of the phases of identified attacks would hinder its success.

Threat Detection an extended version of the Cyber Kill-Chain and have the analysis engine categorizing and mapping suspicious behaviour into these phases, as shown below:

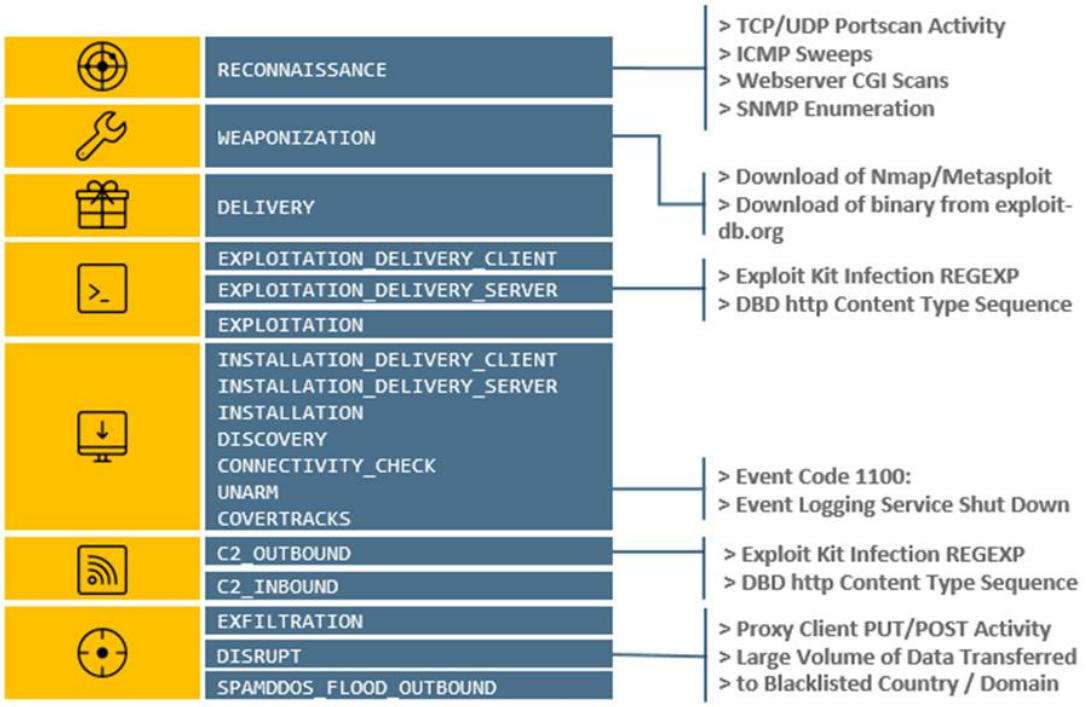


Figure 9 Cyber Kill-Chain

Classifying in accordance with the Cyber Kill-Chain enabled by the analysis engine in the qualification of events, and by the Security Analyst during security validation activities to determine where in the Cyber Kill-Chain phase certain activities were seen and better understand the life-cycle of the incident, impact and risk involved.

Such contextual awareness is used by the analysis engine to identify the relation of suspicious activities by applying a large set of rules and logics both suppressing, but also raising, the threat severity of combined events.

3.3.1.5 Correlation Signatures

Correlation Signatures are used to detect threats and suspicious behaviours spanning over a long period of time, or through multiple events and log sources.

These signatures are typically created to address threats and suspicious activities where the activities and order of execution are known and static in nature.

Using Complex Event Processing (CEP) on cached data (typically configured to >60 days), NTT correlates activities spanning over a long period of time to identify slow behaviour or threats which have stayed dormant before activation.

3.3.2 Correlation

Correlation enables detection of malicious behaviour either spanning over multiple log-sources, or within the same log source over a longer period.

NTT assesses the combined result across all IOCs, anomalies and behaviours by performing real-time correlation of current and historic data, across all client log

sources using both static correlation signatures and dynamic correlation through "Boost" scorings.

3.3.2.1 Boost Scoring

Boost Scoring is a NTT developed detection mechanism that identifies suspicious activities using the combined insights offered by multiple enrolled sources across your estate. This enables detection using activities and events that normally would not be of a significant interest by themselves, but in combination their relevance is strengthened.

By grouping these activities and events on a user and entity basis, Boost Scoring enables identification of suspicious behaviours from the combined insights, and builds up Confidence and threat severity scoring for each group over time.

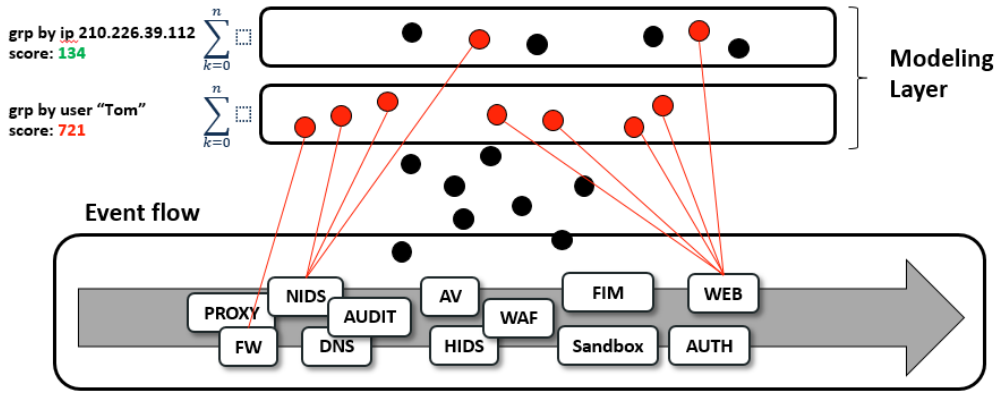


Figure 10 Boost scoring

By keeping the group state for a long period of time (typically >60 days) Threat Detection – Enhanced detects evasive threats that have stayed dormant for a longer period of time from the initial breach where, for example, added activities in this period are considered in relation to the initial infection attempt.

Once a Boost Score reaches a certain level it will be presented to a Security Analyst in the format of a security incident timeline where the combined activities in the Boost Score group are presented to the Security Analyst.

This technique enables detection of dormant threats and slow-moving attacks (a traditional evasion technique) and all suspicious activities are assessed in their entirety regardless of threat severity, time or log source.

3.3.2.2 Asset Aware Analytics

Having contextual understanding of target victims is key in identifying threats, determining the likelihood of a successful attack, and understanding the potential impact.

The usefulness of such contextual information is related to the accuracy and timeliness of the information. Inaccurate or stale information may have the opposite effect, resulting in incorrect false-negatives and the risk that Security Analysts may draw the wrong conclusions.

For the Threat Detection – Enhanced Service, NTT has adapted a combination of manual creation and automated detection techniques to identify monitored assets and associated traits using passive monitoring (Passive Monitored Asset Detection), active probing (Vulnerability Correlation) and manual creation (Manual Monitored Asset Information). Such a combination ensures that the information associated with monitored asset are, and remain, of high quality.

Manual Monitored Asset Information – You provide manual monitored asset information in the Service Transition Workbook used during service transition. The SOC maintain and use this information during continuous service delivery.

Passive Monitored Asset Detection – The Threat Detection analysis engine has built-in techniques to passively identify Monitored Assets and their functional role by monitoring for behaviours in logs analysed.

Vulnerability Correlation – By Integrating with the Qualys platform used in NTT's Vulnerability Management Service, Threat Detection – Enhanced gains a detailed understanding of the Monitored Assets with information of (not limited to) running software, exposed services and vulnerabilities associated to these. See *3.6.4 Vulnerability Correlation (Enhanced Only)* for more information.

The monitored asset information is used by the Threat Detection – Enhanced analysis engine to increase its ability to identify threats and increase accuracy and is presented to the Security Analysts to improve the contextual understanding of threats targeting/or deriving from your estate.

3.3.2.3 Lateral movement identification cross IT/OT environments

Using purpose-built IT/OT detection techniques, Threat Detection – Enhanced monitors OT in combination with IT environments. This approach enables the unique ability to identify initial compromise of IT assets, the lateral movement from the IT environment, to the actual impact on OT assets.

3.4. Threat Detection - Standard Service Features

Threat Detection - Standard is a fully automated service with no Security Analyst interaction. The Service detects threats using Threat Intelligence and Advanced Analytics as described in 3.2 Threat Intelligence and 3.3 Detection Types.

3.4.1 Client Notification

Security Incident Report notifications are sent via email as per the Service Transition Workbook.

3.4.2 Security Analyst interaction

Threat Detection – Standard is an automated service. Security Analysts are not involved in normal service delivery.

3.4.3 Severity and Confidence Settings

Threat Detection – Standard uses machine-learning in identification and reporting of security incidents. As we gain 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, Threat Detection – Standard will start notifying you 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.

Altering the confidence level can significantly increase, decrease, or disable the service's ability to detect emerging, and evasive threats for the benefit/trade-off of increasing, or decreasing the number of false-positives. Refer to 3.4.3.2 Feature Considerations and Cautions for details.

For example, configuring Confidence allow for you to adjust the axis shown as "Confidence" in the below image Note: Image describes the concept, the axis's does not represent actual running configuration:

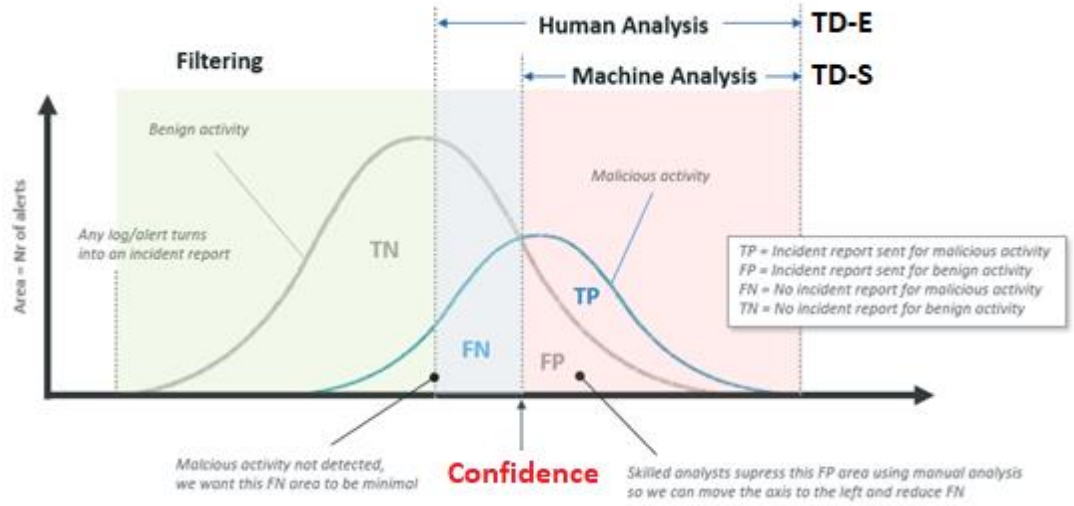


Figure 11 Automated service delivery: False-positive/False-negative threshold tuning

Confidence configuration is performed on a per-Severity (Low, Medium and High) basis. Meaning that you may configure High Severity security incidents, which are relatively uncommon, to require a lower minimum Confidence before it results in client notification, than for Low Severity security incidents, which is very common (e.g. external port scan) to require a much higher level of minimum Confidence (or disabled – recommended).

Severity	Min- Confidence (>=)
High	Medium
Medium	High
Low	Disabled

Table 4 Threat Detection-Standard Default Running Configuration

Example usages and result:

- Suppose Confidence is set to Max on High Severity, then very few (false positive) reports on High Severity threats are likely to be generated. Setting Confidence to Max also means that some threats may go unreported.

- Suppose Confidence is set to Min on High Severity, then more reports on High Severity are likely to be generated. Setting Confidence to Min also means that these threats may occasionally generate false positives and these threats will also be reported.
- Suppose Confidence is set to Disabled on Medium Severity, then all Medium Severity threats would be reported.

3.4.3.1 How to set Confidence and Severity settings

Confidence and Severity configuration are primarily delivered as a self-service functionality on Manage Centre.

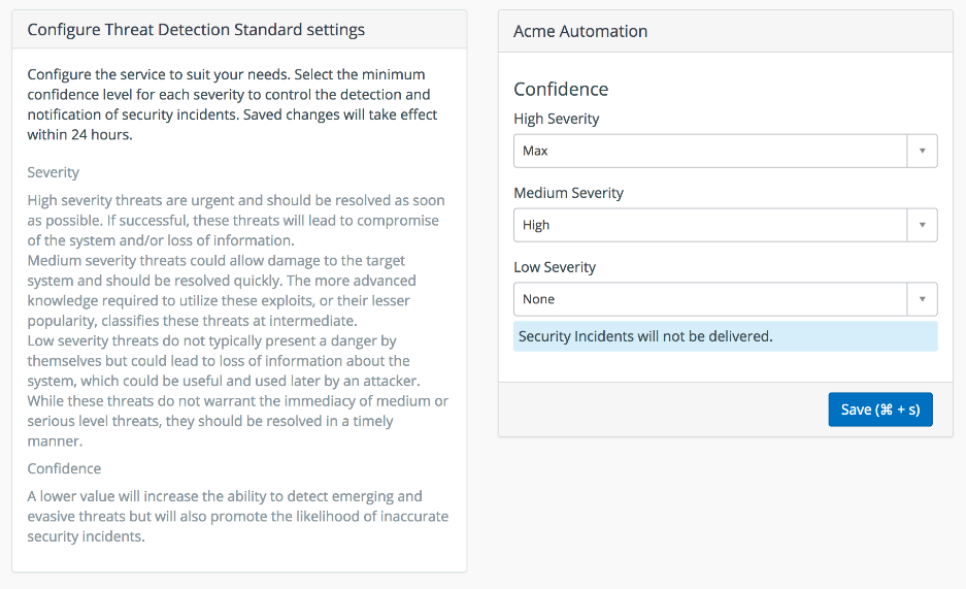


Figure 12 Client Self-service Tuning on NTT's Manage Centre Portal

Alternatively, you can request us to perform the configuration either during service transition in the Service Transition Workbook, or through a request on Manage Centre during continuous service delivery.

3.4.3.2 Feature Considerations and Cautions

- Client Confidence and Severity settings are applied within 24 hours of the change.
- Client changes to our default configuration may have a significant risk of negatively impacting the service experience and may result in:
  - partial de-activation of Threat Detection-Standard capabilities
  - increase of false-positives (inaccurate security incidents), or false-negatives (missed security incidents), and
  - large amounts of security incidents given that Low-Medium Severity security incidents are being relatively common in certain environments.
- Large amounts of security incidents may trigger the Service's flood protection capabilities, resulting in the suppression of future security incidents for the same Severity:

- flood protection is activated on a per-Severity basis. For example, Low Severity security incidents cannot result in the suppression of Medium/High Severity security incidents, and
- flood protection is activated on a 24 hours sliding-window basis.

3.4.3.3 Automated Security Incident Reports

As the threat detection engine identifies security incidents, Threat Detection-Standard provides you with a Security Incident Report. The Security Incident Report includes a detailed description of the threat, identified activity, and impact combined with a generalized recommendation of suitable incident response steps to take in relation to the specific threat.

Typical content

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

The contents of the Security Incident Report 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 Security Incident Report significantly lowers the risks to your business.

Example Threat Detection Standard Automated Incident Report

The following image is an example Security Incident Report with generic recommendations provided:

NTT | Security Incident Report

High

BOOST-D.PCK-005: Malicious behavior threshold exceeded (Internal Source IP)

Customer	Georgia State University	
Device	TYRELLCORP-CTS-3315	
Signature	BOOST-D.PCK-005: Malicious behavior threshold exceeded (Internal Source IP)	
Severity	**Confidence**	**Reference #**
High	High	INC0179420

Date and Time			
Start Date	2020-02-25 17:22:53	**End Date**	2020-02-25 17:30:44

Description

The host 10.22.33.145 has triggered the signature "BOOST-D.PCK-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:

Date/Time	Source IP	Signature	Action	Score
2020-02-25 17:22:53	10.22.33.145	FW-D.PCK-137: Rare privileged outbound connection (TCP outbound)	ACCEPT	150
2020-02-25 17:22:53	10.22.33.145	FW-D.PCK-183: Accepted outbound connections attempts towards rare country (geoip), privileged ports	ACCEPT	20
2020-02-25 17:22:53	10.22.33.145	FW-D.PCK-064: Accepted outbound connections towards rare country (geoip)	ACCEPT	100
2020-02-25 17:23:05	10.22.33.145	DNS-D.PCK-035: Public IP lookup access	ACCEPT	35
2020-02-25 17:23:05	10.22.33.145	TMBP-D.PCK-005: Proxy Client Suspicious IP lookup access	ACCEPT	12
2020-02-25 17:23:05	10.22.33.145	PROXY-D.PCK-034: Suspicious User Agent detected	ACCEPT	80
2020-02-25 17:23:05	10.22.33.145	PROXY-D.PCK-153: Public IP lookup access (URL)	ACCEPT	10
2020-02-25 17:24:05	10.22.33.145	DNS-D.PCK-093: IP lookup requests followed by reputation lookup (allowed)	ACCEPT	35
2020-02-25 17:24:05	10.22.33.145	DNS-D.PCK-095: Reputation lookup (allowed)	ACCEPT	35
2020-02-25 17:28:38	10.22.33.145	FW-D.PCK-216: Allowed outbound connections to distinct malware ports (Trickbot)	ACCEPT	35
2020-02-25 17:30:12	10.22.33.145	PROXY-D.PCK-209: Allowed proxy client session to blacklisted IP (Malware JPN)	ACCEPT	35
2020-02-25 17:30:12	10.22.33.145	PROXY-D.PCK-604: Allowed request for suspected C2_OUTBOUND (HindSight) [TRICKBOT]	ACCEPT	35
2020-02-25 17:30:24	10.22.33.145	PROXY-D.PCK-611: Multiple user-agents noted while communicating with rawIP/similar URL	ACCEPT	195

Event extracts for the 15 alerts are detailed below:

FW-D.PCK-064: Accepted outbound connections towards rare country (geoip) *[Killchain state: C2_OUTBOUND]*

Date/Time	Source IP	Source port	Destination IP	Protocol	Dest port	Action	Country
2020-02-25 17:22:53	10.22.33.145	49811	190.214.13.2	TCP	449	ACCEPT	EC

FW-D.PCK-137: Rare privileged outbound connection (TCP outbound)

Date/Time	Source IP	Source port	Destination IP	Protocol	Dest port	Action
2020-02-25 17:22:53	10.22.33.145	49811	190.214.13.2	TCP	449	ACCEPT

FW-D.PCK-183: Accepted outbound connections attempts towards rare country (geoip), privileged ports

Date/Time	Source IP	Source port	Destination IP	Protocol	Dest port	Action	Country
2020-02-25 17:22:53	10.22.33.145	49811	190.214.13.2	TCP	449	ACCEPT	EC

DNS-D.PCK-035: Public IP lookup access *[Killchain state: DISCOVERY]*

Date/Time	Source IP	Record type	Destination record	Action
2020-02-25 17:23:05	10.22.33.145	A	ipecho.net	ACCEPT

TMBP-D.PCK-005: Proxy Client Suspicious IP lookup access *[Killchain state: DISCOVERY]*

Date/Time	Source IP	Destination URL	Action
2020-02-25 17:23:05	10.22.33.145	hxxp://ipecho[.]net/plain	ACCEPT

Recommendation/Action

Based on the activity noted in this report, NTT recommends the following actions:

Isolate the client*
Isolate the client 10.22.33.145 to contain the suspected compromise. This can be done by disconnecting the host or by blocking further communication from the host (using Firewall, NAC, Proxy or similar system).

Block access to potentially malicious hosts*
Block access to ipecho[.]net and 203[.]176[.]135[.]102 to prevent further interaction with these potentially malicious hosts. Please note that we recommend an impact analysis before blocking communication since this may disrupt services which are critical to your organization.The block action needs to be taken on all applicable gateway appliances (Firewall, Proxy or similar system) in order to be effective.

Log file investigation
Investigate and attempt to identify any additional outbound connections from the client 10.22.33.145 from the time of the above activity. Typically this would include searching through logs from sources such as Proxy, Firewall and DNS. Please make sure that the logs are correctly timestamped (timezone/NTP) so that the relevant logs are covered by the searches.

Perform an offline antivirus scan
Make sure to update the client antivirus software and perform a full scan of the host, preferably while disconnected from the network. Note that many antivirus vendors are unable to detect the latest Exploit Kits (EK) commonly used by malware, so we also recommend to upload any suspicous files found to a security vendor for sandbox evaluation.

Rebuild the client host*
If the malware activity can be confirmed for the client host 10.22.33.145 we strongly recommend to reimage the host to make sure all traces of malware is removed.

Figure 13 Threat Detection – Standard Sample of Automated Incident Report

3.5. Threat Detection - Enhanced Service Features

Threat Detection - Enhanced uses Advanced Analytics and Threat Intelligence to detect threats that are further investigated by Security Analysts using dedicated tools for event driven threat hunting and threat validation.

3.5.1 Client Notification

The Security Analyst prepares the Security Incident Reports based on detailed investigation and threat hunting. You are notified about security incidents based on

your selection of NTT-supported notification options. Each notification option is configurable on a per-contact and severity basis.

Notification option availability

- **Critical Severity;** Phone / e-mail notifications
- **Low, Medium, High Severity;** E-mail notifications

For security reasons the notification (e-mail / phone) will only notify you of the Security Incident and refer you Manage Centre for details.

Phone notification details

Clients with phone notifications must provide us with a prioritized list of client contacts. This list may contain 3 (three) or less client contacts with phone notifications selected.

We consider the client phone notification complete once any of the client contacts have been reached. No additional contacts are called.

If we are unsuccessful in reaching your client contacts, we will repeat the attempt a second time. If the second attempt also is unsuccessful we consider the phone notification failed and no further attempts are made.

3.5.2 Security Analyst Interaction

3.5.2.1 Detailed Security Incident Investigation

Events qualified by the analysis engine (or that of reliable signatures triggered by monitored technologies), are presented to the Security Analysts within the NTT propitiatory threat hunting and threat validation framework called Analyst Workbench.

Figure 14 Security Incident investigation life-cycle

Within this framework the Security Analysts are provided with all the event information, the holistic insights across client-monitored sources, and strong threat hunting and threat validation capabilities across:

- Threat Hunting – Analyst Workbench, Big Data

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

3.5.2.2 Event-driven Threat Hunting

Security Analysts perform event-driven threat hunting activities as part of security incident validation in the Threat Detection - Enhanced Service. 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 your entire monitored estate and the ability to perform threat hunting activities across these in a responsive manner, provides further insight into the entire security incident life-cycle.

A view enabled by supporting tools, contextual data and insights into your sources result in the Security Analyst's ability to offer accurate, relevant and actionable Security Incident Reports.

3.5.3 Vendor Integration and Evidence Collection

The Threat Detection - Enhanced 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 and signature information) describes that something suspicious has happened and 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 IOCs and behavioural information in a Sandbox Execution Report. 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.

SYSLOG event (typical output stored in a SIEM)	Same event, now combined with PCAP data from the *Threat Detection Service*
2017-12-08T21:35:09;83.123.221.23; 80; 192.168.10.10; 23491; virus; 191338785; Trojan/Win32.docdl.ltl; allowed	2017-12-08T21:35:09;83.123.XXX.XX; 80; 192.168.10.10; 23491; virus; 191338785; Trojan/Win32.docdl.ltl; allowed *GET /***M2z/ HTTP/1.1* *Host: ****.com* Connection: Keep-Alive HTTP/1.1 *200 OK* Date: Thu, 07 Dec 2017 06:06:50 GMT Server: *Apache* X-Powered-By: PHP/7.0.26 Pragma: no-cache Content-Disposition: attachment; filename="*0926.exe*" Content-Transfer-Encoding: *binary* Transfer-Encoding: chunked Content-Type: application/octet-stream 11ff8 MZ.....@.....!..L.!This program cannot be run in DOS mode.

Figure 15 Syslog Compared to Threat Detection Enhanced Evidence Collection

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 configuration guide for specifics). Typical methods, i.e. Integration point (examples) include:

- API (preferable)
- HTTPS
- Streaming, and
- Database

3.5.3.1 Security Incident Reports

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.

Security Incident Report Content

- *Estimated Threat Severity:* the Security Analysts assign an appropriate threat Severity based on their analysis and assessment, which is an indication of the impact of the threat on your estate.
- *Analysis Summary:* contains information such as threat category, first and last time the threat has been observed, etc.
- *APT (Advanced Persistent Threat):* if the security analyst concludes that the threat is an APT, the APT symbol is enabled in the report.

- *Leakage:* the Leakage symbol is enabled if the security analyst verifies sensitive data leakage during investigations.
- *Incident Details:* graphical visualization of the steps of the attack.
- *Incident Description:* Security Analysts describing the threat life-cycle and detailing how and on what basis the threat was identified.
- *Recommendations:* a set of actionable response suggested by the Security Analysts for remediation.
- *Alert Data: d*etailed list showing sources and alerts triggered which contributed to the identification of the security incident.

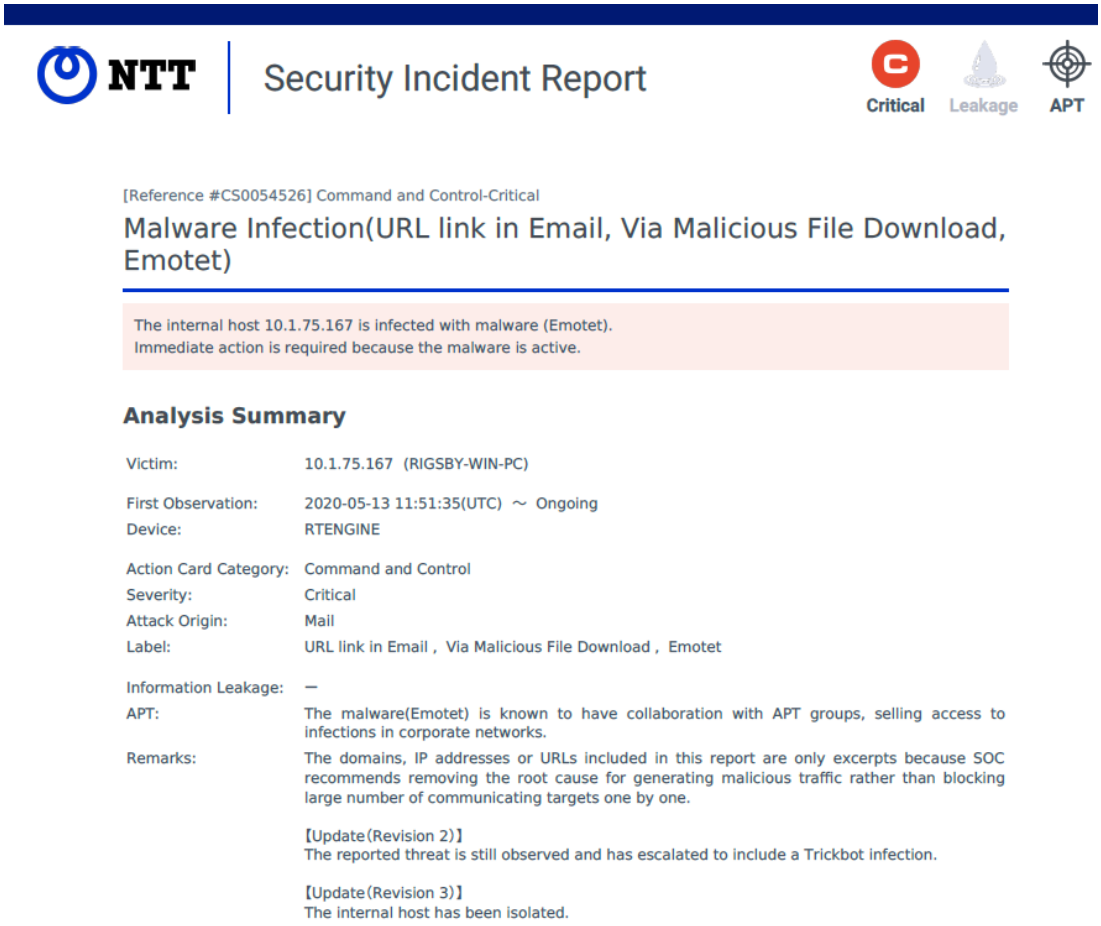
The contents of the Security Incident Report significantly increases your ability to take swift and informed steps in resolution of escalated security incidents.

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 Security Incident Report significantly lowers the risk to your business.

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

Validated security incidents are categorized with appropriate threat Severity based on the SOC team's analysis and assessment.

If you are subscribed to NTT Proactive Response and/or Remote Isolation services, the Security Incident Report will contain information relevant to these service options.



NTT | Security Incident Report

Critical Leakage APT

[Reference #CS0054526] Command and Control-Critical

Malware Infection(URL link in Email, Via Malicious File Download, Emotet)

The internal host 10.1.75.167 is infected with malware (Emotet).
Immediate action is required because the malware is active.

Analysis Summary

Victim:	10.1.75.167 (RIGSBY-WIN-PC)
First Observation:	2020-05-13 11:51:35(UTC) ～ Ongoing
Device:	RTENGINE
Action Card Category:	Command and Control
Severity:	Critical
Attack Origin:	Mail
Label:	URL link in Email , Via Malicious File Download , Emotet
Information Leakage:	—
APT:	The malware(Emotet) is known to have collaboration with APT groups, selling access to infections in corporate networks.
Remarks:	The domains, IP addresses or URLs included in this report are only excerpts because SOC recommends removing the root cause for generating malicious traffic rather than blocking large number of communicating targets one by one. 【Update(Revision 2)】 The reported threat is still observed and has escalated to include a Trickbot infection. 【Update(Revision 3)】 The internal host has been isolated.

Figure 16 Threat Detection Enhanced Sample of Security Incident Report

Please refer to Appendix A for the complete sample security incident report.

3.6. Service Options

3.6.1 Cyber Threat Sensor (Enhanced Only)

Threat Detection – Enhanced clients have the option to add NTT's managed Cyber Threat Sensor (CTS).

The CTS is purpose-built for Threat Detection – Enhanced, using a combination of Advanced Analytics, traditional detection techniques, and Threat Intelligence to identify sophisticated threats on a network layer.

Through the recording of all monitored traffic (full PCAP), the CTS captures large quantities of evidence data in relation to identified threats.

As events are generated the CTS sends these and all associated evidence data upstream to the SOC where it is seamlessly made available in the Analyst Workbench, providing the Security Analyst with the evidence/traffic data needed to perform deep network investigations.

Clients subscribing to multiple CTS devices also benefit from cross device correlation, a feature that brings the insights of each running CTS instance together through the correlation of both suspicious activities and threats as these

are identified by any running CTS instance. This allows for the total sum of activities to be analysed, improving the ability of the Service to identify threats moving laterally across the monitored networks.

The combined detection techniques, cross device correlation, and evidence gathering capabilities of the CTS increases the ability of the Service to accurately identify and validate threats, and investigate the impact of these.

The CTS enables threat detection capabilities on the network layer and can be subscribed to standalone without ingesting any regular log sources (e.g. FW, Proxy, etc.) into the Service. However, it is recommended to combine CTS devices with monitoring of your security infrastructure and additional log-sources, augmenting the detection capabilities and placement of these.

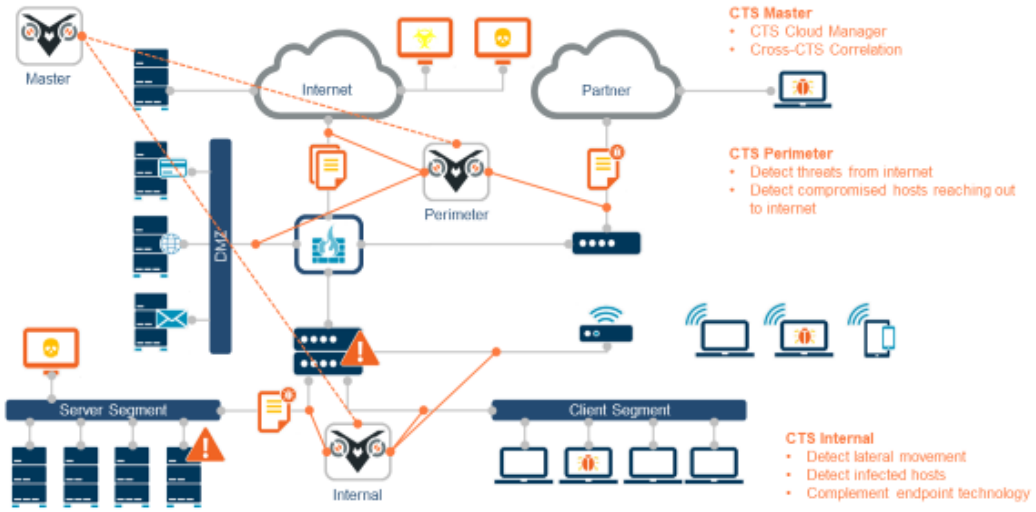


Figure 17 Cyber Threat Sensor placement

Example CTS Usages

- Add NTT's proprietary Advanced Analytics threat detection capabilities on the network layer.
- Add deep network investigations (full PCAP), increasing the ability of the Service to validate threats and the impact of these.
- Extend the reach of Threat Detection – Enhanced into your network (reduce service blind spots).
- Cross device correlation to improve the ability of the Service to detect threats moving laterally across your networks.

3.6.1.1 Service Option Variants

The CTS service option is available in the following two variants:

- CTS Perimeter:

- Monitors your networks with CTS Perimeter (e.g. internet breakout, DMZ), delivering Threat Detection – Enhanced monitoring of client traffic towards and from the Internet.

- CTS Internal:
  - Monitors your internal networks to improve detection of threats moving laterally across internal assets, and threats of internal origin by removing service blind spots.

CTS Internal sensors must always be combined with CTS Perimeter (at Perimeter) when client assets can be connected towards the Internet.

Incorrect Placement of CTS Internal

NTT reserves the right to audit the CTS deployment network location (Internal versus Perimeter). If NTT deems the traffic monitored to be in conflict with the deployment location, you are responsible to work with NTT in updating the Purchase Order and changing the CTS sensor type accordingly based on the results of NTT's audit of the CTS deployment network locations.

3.6.1.2 Service option pre-requisites

You are responsible for providing the systems (hardware, or virtual) and performing the initial system preparations in accordance with specifications and instructions detailed in the *NTT Cyber Threat Sensor Installation and Configuration Guide* that will be provided to you during service transition, including:

- procuring and maintaining the required hardware and support, or provision virtual environment in accordance with NTT's specifications
- performing operating system and software base installation on your system in accordance with NTT's instructions
- providing the CTS with end-to-end connectivity in accordance with NTT's connectivity details
- configuring suitable network capabilities to mirror/span in-scope traffic to the CTS listening port(s)
- ensuring that mirrored traffic reflects the type of subscribed CTS *(see 3.6.1.1 Service Option Variants)*.
- ensuring that mirrored traffic is within the bounds of maximum throughput (1 Gbit/s)
- providing a Point of Contact whenever there is a need for on-site assistance as deemed suitable by NTT (typically during service transition, or in response to an availability-related incident).

3.6.1.3 Service Option Features

Cyber Threat Sensor Capabilities and Service Features
Threat Detection Capabilities
Advanced Analytics (machine learning / behavioral modeling) on Network Layer
Threat Reputation and Pattern Signature Matching on Network Layer

Cyber Threat Sensor Capabilities and Service Features
Cross Device Correlation (Lateral Movement)[2]
Enhanced by NTT's Global Threat Intelligence Center
Continuous Threat Intelligence updates driven by production investigations
Evidence data (Full PCAP)
Management Service Elements
Operating System/Software Management
Health and Availability Monitoring
Health and Availability Incident Management
Capacity Management
Decommissioning

Table 5 Cyber Threat Sensor Capabilities

3.6.1.4 Threat detection capabilities

The CTS device identifies threats by analysing traffic on your networks using NTT's Threat Detection Analysis Engine (see *3.2 Threat Intelligence*, *3.3 Detection Types* for details).

Clients subscribing to multiple CTS devices benefit from Cross Device Correlation. Identified suspicious activity, or threats are cross-correlated between running CTS devices to detect lateral movement in your network.

Upon identifying suspicious activities, or threats, the CTS provides the Security Analyst with evidence data (full PCAP), allowing for deep network investigations. The added evidence data increases the ability of the Service to analyse, validate and escalate security threats.

3.6.1.5 Operating System/Software Management

We maintain the supported operating system and installed software on CTS devices. We performed maintenance remotely and at our sole discretion, typically as relevant security hotfixes are made available, or as part of standard operating system software management.

3.6.1.6 Health and Availability Monitoring

We monitor CTS devices for key performance indicators of resource utilization to determine the overall health, performance, and availability. The CTS also regularly triggers and monitors for heartbeat events used to validate the sensor's end-to-end functionality. The CTS service option automatically generates incidents in the ITSM system based on the events which exceed thresholds against specific poll cycles of key metrics. The SOC engineer investigates and analyses the events to determine a potential corrective or control action to resolve the related incident. See *3.6.1.7 Health and Availability Incident Management* for more information.

[2] For Clients subscribing to multiple CTS devices

Upon identifying health and availability-related issues which risks our ability to monitor your estate for threats, you will be notified and kept up to date with the overall health and availability via the incident ticket available on Manage Centre.

Health and Availability Improvement and Recommendation

We utilize standard poll cycles and thresholds when monitoring CTS and may adjust the thresholds based on the historical data collected to eliminate unnecessary events from occurring. With this data, we may identify potential methods of improving CTS performance and overall health and availability.

Health and Availability Change Implementation

Changes to running software on CTS devices to resolve identified health and availability issues are performed at our sole discretion outside of any eventual client change management process.

3.6.1.7 Health and Availability Incident Management

Incident management focuses on responding to any unplanned interruption to the Service and CTS operation to minimize any impact on service quality and availability.

Incident Generation

Incidents may be generated through health and availability monitoring by us, and made available in Manage Centre.

Incident Resolution

We will work with you to resolve the incidents and move them to a *resolved* state in Manage Centre to allow you to confirm resolution. Incidents will then remain in a *resolved* state until you:

- confirms resolution - the incident will be moved to a *closed* state
- do not respond - the incident will be automatically closed after 10 days

Incident Reporting

We will notify you of all incidents via a notification email, which contains very minimal information for security purposes, Full incident details will be available via Manage Centre.

3.6.1.8 Capacity Management

Capacity Monitoring and Reporting

The monitoring systems utilized by the CTS regularly check a number of telemetry points. Through continuous monitoring, we are able to highlight potentially impacting trends. This can be useful for determining if there is a problem that needs to be addressed or if the configuration items are becoming oversubscribed. For example, CTS receiving more traffic than sizing allows. Using this as a starting point for incident management, we will work with you to advise on potential resolution or mitigate the risk.

Capacity Improvement Recommendation

Where NTT monitoring determines that a device is oversubscribed, we will work with you to determine the best plan and path forward. Examples include but are not limited to:

- requesting you to change your network architecture
- requesting you to update hardware/assigned virtual resources or licenses to facilitate greater capacity

The CTS device maximum throughput is an estimation based on averages, and is not to be considered a guarantee of throughput. Your environment variables may result in the CTS delivering higher throughput, but also lower than that detailed by the specifications.

You are responsible for adhering to our recommendations, and accepting the potential risk of not doing so, for example service degradation, or blocking our ability to provide service delivery.

Capacity Planning

In support of continued development of the CTS, we may make decisions about future requirements and detail these in the *NTT Threat Detection CTS Installation and Configuration Guide*. This provides invaluable forward planning to those responsible for budgeting or capacity planning.

Capacity Change Implementation

Through the consistent and uniform measurement of telemetry from the CTS, we can make recommendations or raise a Request for Change (RFC) to be approved by you to enhance or avoid future capacity issues that may arise. This is subject to the necessary approvals and the advice being followed. Any capacity issues related to hardware refresh, virtual resources or design are not in the scope of this service.

3.6.1.9 Decommissioning

Upon service decommissioning, you must maintain connectivity to each running sensor instance until we have confirmed decommissioning completion. This allows us to clean systems from NTT proprietary software. Upon completion, we will hand the decommissioned systems back to you.

3.6.2 Client Enriched and Aggregated Log Search (Enhanced Only)

The Investigator Tool **('Investigator')** provides cloud-based, real-time access to log data. As we collect and analyse logs, it also archives a copy of the logs in a secure, cloud-based repository. Online access to enriched and aggregated logs through Manage Centre is enabled without the need for additional on-premise equipment or an up-front capital investment. This accessibility enables data mining of the logs for efficient security and compliance with incident investigations.

Threat Detection - Enhanced clients have the option to include our Investigator log search capabilities. Investigator provides you with access to an interface to perform historical log searches from our Manage Centre Portal.

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

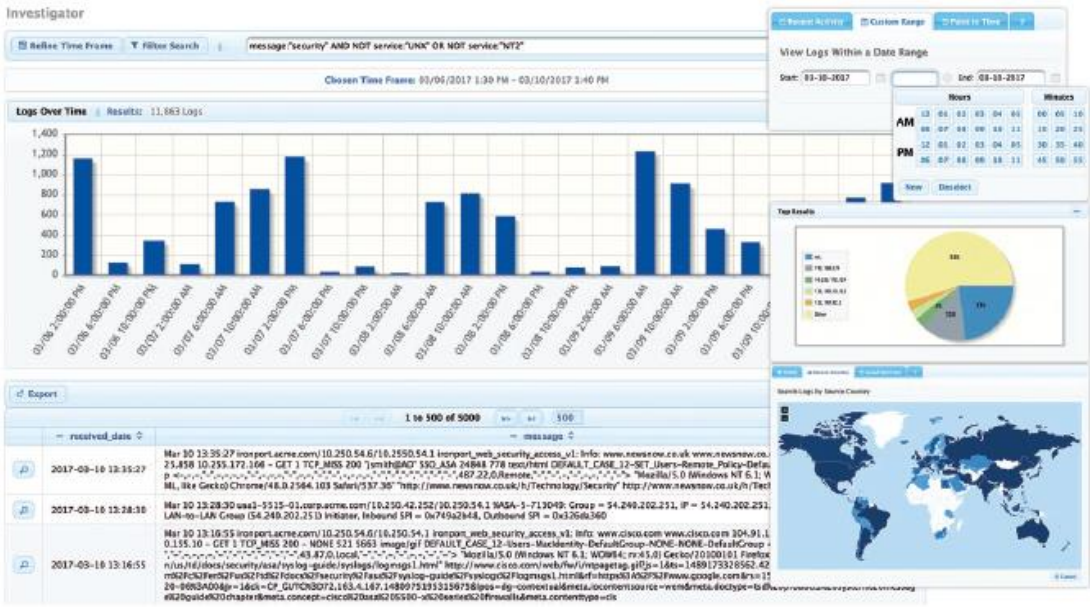


Figure 18 Investigator

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 your security team to immediately investigate security incidents instead of spending time locating and accessing necessary logs.

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.

3.6.3 Secure Long-Term Log Storage

You have the option to purchase Secure Long Term Log Storage (SLTLS), available with both Threat Detection – Enhanced and Standard.

SLTLS utilizes the MSS infrastructure to store and retrieve raw logs collected by the platform. SLTLS will store logs for all devices in scope for your subscribed monitoring service. SLTLS is not customizable to specific devices or IP addresses.

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 your 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 you can perform raw log searches. The user interface is located within the Manage Centre Portal. You may specify a date range along with an IP address as required input for log searches. Results from searches

are displayed in the Manage Centre 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 you with the ability to self-service search for raw logs via the Manage Centre Portal. As this is a self-service offering, you are responsible for performing searches and downloading relevant log files.

3.6.4 Vulnerability Correlation (Enhanced Only)

Threat Detection - Enhanced clients subscribed to the Vulnerability Management Service may benefit from added vulnerability correlation capabilities on an opt-in basis.

A feature opt-in request is made during service transition, or raised by you via Manage Centre during continuous service delivery.

Upon opt-in, the Vulnerability Management Service provides Threat Detection - Enhanced clients with added contextual information of your assets and vulnerabilities which increase the Security Analyst's overall ability to understand the relevance of a threat and raise the accuracy of Security Incident Reports.

Service option prerequisites:

- Threat Detection - Enhanced clients must also be 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 reflects the size of the organization and its asset estate. Smaller subscriptions may result in limited usages caused by Qualys API restrictions.

Note: Threat Detection Enhanced Service will only be using the information provided by NTT's Vulnerability Management Service in relation to analysing security threats. For reporting and management of vulnerabilities and configuration bad practices, refer to the Vulnerability Management Service.

Following are examples of information which may be made available to Threat Detection - Enhanced clients by opt-in to the Vulnerability Correlation Service. Specifics depend on asset configuration and running services:

- **Asset information**
  - DNS Hostname
  - NetBIOS Name
  - OS Information
  - Last Vulnerability scan
  - First Found
  - And more.
- **Vulnerabilities**
  - First Detected

- Last Detected
- Service Modified
- CVSS Base
- CVSS Temporal
- Threat Information
- Impact
- Solution
- Exploitability
- Associated Malware
- And more

- **Improper software configurations**
  - Correlating such contextual information with the events undergoing analysis and their associated descriptions (e.g. reg-exp, pattern, CVE, CVSS) and evidence (PCAP, sandbox executional trace) assist the Security Analyst to determine the extent of the potential threat in your environment.
- **Likelihood of success**
  - Is the target victim vulnerable for the exploit used?
- **Indication of being targeted**
  - Was the attacker targeting the running software of the host?
- **Alternative attack surfaces**
  - Is the victim running additional services with exposed vulnerabilities?
  - Is the victim running bad configuration that could exploited the attacker?
  - Do you have additional exposed hosts with the same weakness successfully exploited?

3.6.5 Proactive Response (Enhanced Only)

Threat Detection - Enhanced clients have the option to purchase the Proactive Response service option. With the Proactive Response option we will take actions to contain/disrupt threats described in security incidents when the Security Analyst deems it appropriate. Actions are performed on your network devices, typically hindering, or limiting the progress of identified attacks sufficiently to provide you with additional time to take informed incident response actions.

Client network devices are subscribed to the containment feed by following instructions provided in NTT's Configurations Guides. Once subscribed, these devices will continuously poll the containment feed for new IOCs (such as IPs, URLs and Domain) and quickly apply additions as blocking rules, resulting in either the disruption/or containment of the threat. This reduces the impact and risks of security incidents identified by Threat Detection - Enhanced.

This option does not include remediation actions, processes or procedures that may occur following responsive actions to contain/disrupt threats.

Option Benefits

- **Cross Client benefits:** You can use all IOCs that are found in Threat Detection - Enhanced for all NTT clients beside your individual IOCs.
- **Orchestration**: Using orchestration techniques, your containment feed is swiftly updated with relevant IOCs, significantly reducing the time threats goes unchallenged from the time of identification.
- **Initial blocking:** Blocking of IOCs seen in association with identified security incidents on a network level, resulting in the containment, or disruption of the threat.
    - While not to be considered replacement for incident response, the swift initial containment/disruption enables client incident response with additional time to take informed steps in incident resolution.

Supported IOC Types

Proactive Response supports containment of threats using a variety of IOC types. Depending on specific needs, capabilities and risks you may choose which types are to be used for containment. The Security Analyst will then, upon identifying a threat, use these IOC types to the best extent to either disrupt, or contain the attack.

IOC types

- To be used on devices with a URL filtering function
    - URLs
    - Domain
- To be used on devices with a Firewall function
    - IPv4 (Dst)
    - IPv6 (Dst)

To get a complete overview on which IOCs are supported on what devices and if any limitations applies for the device, see the detailed Configuration Guide.

Client Acceptance

- You accept that Proactive Response actions are of an emergency change nature and are considered outside traditional change management processes in priority of disrupting/containing threats.
- You understand and accepts the risks associated with responsive actions and the potential negative impact it may have on the availability of your environment.
- We will not be held liable for any negative impact responsive actions within the scope of Proactive Response service option may have.

Service Option Prerequisites

- Your network devices are configured in accordance with the Configuration Guide.
- Your network design and your security policy shall be configured in a manner which supports the containment actions provided by us.

- Your network devices are provided with access to the security incident response platform using Internet connectivity.

3.6.6 Remote Isolation (Enhanced Only)

Threat Detection - Enhanced clients have the option to purchase the Remote Isolation service option. With Remote Isolation, we take actions to isolate compromised/malicious host endpoints following Security Analyst validation. Remote Isolation actions are performed using the isolation capabilities of the in-scope Endpoint Detection and Response (EDR) technology, resulting in isolation of target host endpoints. This enables you to focus your resources on post-isolation remediation and incident response actions. We inform you of any Remote Isolation actions taken in the Security Incident Report.

Option Benefits

- **Host Endpoint Isolation:** Remote Isolation allows for compromised / malicious endpoints to be isolated from your network, and in some cases (depending on EDR technology) result in a complete lock-down of the target endpoint. While not to be considered replacement for incident response, the swift initial isolation of the endpoint enables you to increase the amount of time available for incident response and incident resolution steps.
- **Automation/Orchestration:** Using various automation and/or orchestration capabilities, your endpoints are swiftly isolated once the Security Analyst have deemed it appropriate. This significantly reduces the time threats goes unchallenged from the time of identification.

This service option does not include remediation actions, processes or procedures that may occur following NTT isolation of compromised/malicious endpoints.

4. Service Management

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 organization with insight to enable your business decisions.

4.1. Service Desk

Our regional Managed Service Center (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, and
- directly reported by Security Operations Centres (SOCs) via our integrated service desk.

4.2. Service Level Management

As a client of NTT's Managed Security Services you will be assigned a Service Delivery Manager.

Depending on the complexity and/or size of your environment, and the mix of products and services, we may recommend contracting a Technical Account Manager (TAM) function as described in 4.2.2 below.

4.2.1 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 Service.

NTT will assign a Service Delivery Manager (SDM) in the contracting region 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 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, and
- service review meeting.

4.2.2 MSS Technical Account Manager (Optional)

The MSS Technical Account Manager is a security management function that provides technical and risk-based oversight and advocacy services for you. The Service is delivered through the MSS Technical Account Manager Team who assign and designate Technical Account Managers to clients who subscribe to the Service providing the full depth and breadth of our cybersecurity capabilities.

The MSS Technical Account Manager Team leverages security best practices and an expansive knowledge base to deliver globally consistent security programs tailored to your specific needs and regulatory requirements. They are committed to developing long-term relationships with you to gain a deep understanding of your business objectives. This includes understanding your strategic initiatives, risk profile by industry or sector and cybersecurity maturity level assessments. This knowledge and level of technical engagement ensures you benefit from an optimized service aligned with your organization's business imperatives.

The MSS Technical Account Manager Team are an additional component of our MSS delivery model, and provide cybersecurity insights beyond MSS. Coupled with our 24/7 SOC teams, the MSS Technical Account Manager Team provides operational support and consultative guidance in alignment with your business priorities and technology roadmaps.

The MSS Technical Account Manager Team provides increased client intimacy by being available on-site (if geo permits) as needed to provide technical guidance and to operate as an extension of your security team. You can benefit from MSS Technical Account Manager Team support of internal and external stakeholder management while they face challenges implementing security controls across your enterprises.

The MSS Technical Account Manager Team are the client advocates who identify and track action items and service requests that have been raised via the service desk to reduce the time to respond to your requests. The MSS Technical Account Manager Team also provides a quality control function to ensure delivery excellence, maintain high levels of client satisfaction, achieve project success, and drive continual service improvement.

The SOC provides 24/7 support and although the MSS Technical Account Manager Team are not a 24/7 resource, the MSS Technical Account Manager Team is included in the escalation path for security incidents whereby intimate knowledge and proximity to you provides further context to aid in assessment and response activities. Overall, the team share observations and makes recommendations to improve your cybersecurity maturity and help you to manage risk.

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.

Our Service Transition Manager is responsible for managing the transition process with you and your organization. As part of the service activation process, the required tools and systems are set up and activated for the managed service to go live.

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

Appendix A Sample Incident Report

NTT | Security Incident Report

Critical Leakage APT

[Reference #CS0054526] Command and Control-Critical

Malware Infection(URL link in Email, Via Malicious File Download, Emotet)

The internal host 10.1.75.167 is infected with malware (Emotet).
Immediate action is required because the malware is active.

Analysis Summary

Victim:	10.1.75.167 (RIGSBY-WIN-PC)
First Observation:	2020-05-13 11:51:35(UTC) ～ Ongoing
Device:	RTENGINE
Action Card Category:	Command and Control
Severity:	Critical
Attack Origin:	Mail
Label:	URL link in Email , Via Malicious File Download , Emotet
Information Leakage:	—
APT:	The malware(Emotet) is known to have collaboration with APT groups, selling access to infections in corporate networks.
Remarks:	The domains, IP addresses or URLs included in this report are only excerpts because SOC recommends removing the root cause for generating malicious traffic rather than blocking large number of communicating targets one by one. 【Update(Revision 2)】 The reported threat is still observed and has escalated to include a Trickbot infection. 【Update(Revision 3)】 The internal host has been isolated. 【Update(Revision 4)】 【Update(Revision 2)】 The reported threat is still observed and has escalated to include a Trickbot infection. 【Update(Revision 3)】 The internal host has been isolated. 【Update(Revision 4)】

Recommendations

Review the associated logs and consider implementing the following recommendations in accordance with your policy.
It is left to the customer to identify the origin of the communication if the victim is a proxy server, a network device or a device with dynamic IP address.

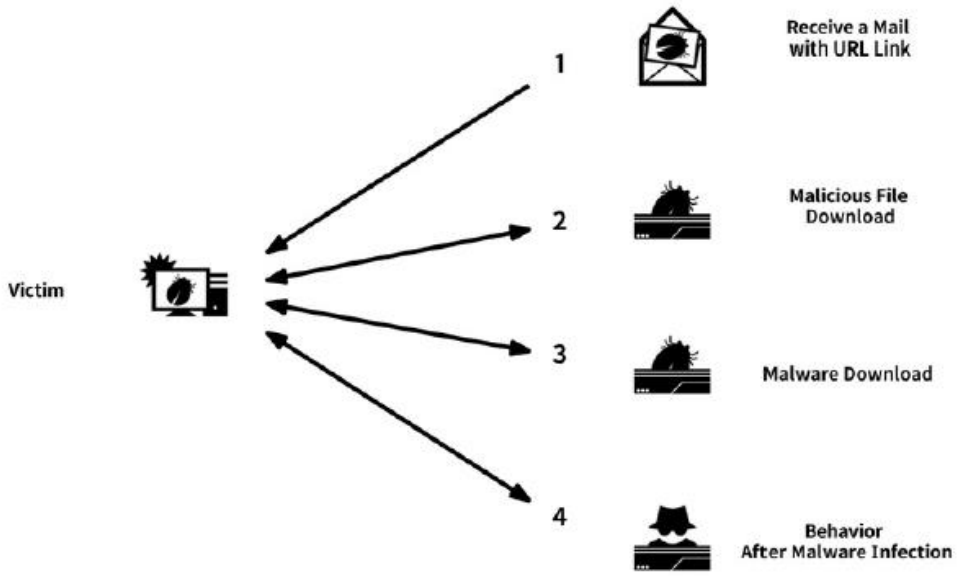
Recommendations

- Isolate the victim host from the network in order to prevent spreading. (SOC performs a isolation process for customers who subscribe to EDR services.)
- Perform a clean installation of the operating system.
- Configure the signatures listed in "Signatures Recommended for Blocking" to blocking mode in your security device.
- If necessary, conduct a further investigation to determine the extent of damage.

NTT | Security Incident Report

Critical Leakage APT

Incident Details



Attack Stages (DE:Detected B:Blocked N:No Log Data)

1	Receive a Mail with URL Link	N
2	Malicious File Download [Malicious File Download Site] • cosmoservicios[[.]]cl	DE
3	Malware Download [Malware Download Site] • bsrcellular[[.]]com	DE
4	Malware Infection [Traffic Destination After Malware Infection] • 87[.]66.13.80	DE

NTT | Security Incident Report

Critical Leakage APT

Incident Description

The victim host, 10.1.75.167 is infected with malware.
10.1.75.167 has been identified by NTT Passive Asset detection as Rigsby-Win-PC.
Rigsby-Win-PC is based on traffic flow analysis identified as an Windows Client PC with Business Criticality - Low.

The starting point of the attack was a malicious link in an email.

Our analysis show that the user visited the malicious website cosmoservicios[.]cl and downloaded a microsoft word file.
The .doc file contains a macro that when activated downloads the full malware from the website bsrcellular[.]com.
We have analyzed available logs and found requests towards the bsrcellular domain to download an .exe file.

Shortly after the .exe download, Emotet command and control traffic could be seen towards 87.66.13[.]80

Emotet is a type of banking malware. It attempts a fraud use of online banking and credit card transactions. It downloads attack modules to expand its capabilities. A function of spreading malware spam has been observed.

Update 2020-05-14 15:00:
The internal host 10.1.75.167 has triggered additional signatures indicating further infection.
Two files named "table.png" and "radiance.png" were downloaded from the IP 192.161.54[.]60, this IP is a known host used to distribute payloads for the Trickbot botnet. The TD-SOC downloaded the files from the external host and could confirm in a sandboxed environment that they are trickbot binaries.
Shortly after these files were downloaded, command and control traffic towards Trickbot C2-servers was identified.
In the outbound traffic, sensitive information about the internal host such as account information, running processes and corporate domain information was seen.

Based on available Threat Intelligence information about Trickbot, likely next steps taken by the threat actors would be:
Lateral movement
Data Exfiltration
Deployment of further malware

More information about Trickbot and its playbooks can be found here:
https://technical.nttsecurity.com/post/102fhgo/analyzing-the-botnet-infrastructure-and-threat-actors-behind-trickbot
https://technical.nttsecurity.com/post/102fsp2/trickbot-variant-anchor-dns-communicating-over-dns
https://technical.nttsecurity.com/post/102fnog/targeted-trickbot-activity-drops-powerbrace-backdoor

Update 2020-05-14 21:50:
New Trickbot activity has been noted from the internal host 10.1.75.4.
10.1.75.4 has been identified by NTT Passive Asset detection as PIXELSHINE-DC.
PIXELSHINE-DC is based on traffic flow analysis identified as an ActiveDirectory and Domain Control Server with Business Criticality - Critical.
PIXELSHINE-DC is also mentioned in the latest Qualys scan report as vulnerable to CVE-2017-0144, commonly known as EternalBlue.

The Threat Actors behind Trickbot has been known to utilize EternalBlue to move laterally internally in the network.

The NTT SOC has taken action in accordance to SLA and isolated the internal host 10.1.75.4 (Proactive Response).

Figure 19 Threat Detection Enhanced Security Incident Report

Appendix B Service Level Agreements

Category	Description	Priority	SLA	Service Credits	Service Credit Limit	Service Calendar
Request Response	NTT will assign a Service Request with priority ____ within ____ minutes of receiving the ticket at NTT`s Service Desk.	P1&P2	60 Mins	5% of Monthly Service Fee	N/A	N/A
		P3&P4	4 Hours			
Request Complete	NTT will resolve a Service Request with priority ____ within ____ minutes of receiving the ticket at NTT`s Service Desk.	P1	2 Business days	95% Service Units of the Request	95% Service Units of the Request	N/A
		P2&P3	5 Business days			
		P4	10 Business days			
Incident Management - Reported	NTT will notify the client of a Security Incident ticket within ___ minutes of the service analysis engine creating a reportable security incident.	N/A	15 Min	N/A	N/A	

Table 6 – Service Level Agreements

Appendix C