Client Service Description

Enterprise Security Monitoring Services

06 October 2020 | Document Version 1.8

NTT contact details

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

FirstName LastName - Services Product Portfolio Director - Security, 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shall be binding on the parties for a period of five (5) years from the issue date stated on the front cover unless superseded by confidentiality provisions detailed in a subsequent agreement.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:	Jason Breytenbach	Security Product Manager - AU	20 Sep 2018
Updated	Mike Oberholtzer	Sr. Product Architect	01 Feb 2019
Updated	Bob Gordon	Portfolio Director - Security	05 Jun 2019
Updated	Sharon Witheriff	Technical Writer	06 Jun 2019
Updated	Bob Gordon	Portfolio Director – Security	02 Aug 2019
Updated	Tore Terjesen	Director	23 Dec 2019
Updated	Tore Terjesen	Director	06 Oct 2020

Release

Version	Date Released	Pages	Remarks
1.3	05 Jun 2019		Internal DRAFT
1.4	06 Jun 2019		Internal DRAFT
1.5	01 Oct 2019		Rebrand
1.6	13 May 2020	All	Updated to reflect the latest Service Description
1.7	06 October		Added Cloud (AWS and Azure) support New Cloud Inventory Report
1.8	20 Nov 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

Ensuring compliance with tightening regulations is key to an effective security strategy, but most organizations have a long way to go to achieve continuous monitoring of networks. Too often, the burden placed on internal teams to monitor systems 24/7 results in gaps in security monitoring or the complete failure to monitor logs at all. Regulations such as PCI DSS and HIPAA demand that logs are regularly monitored, and failure to do so can result in stiff penalties.

Our Enterprise Security Monitoring (ESM) Services provide you with 24/7 log monitoring and analysis so you can comply with robust log monitoring requirements. If the ESM analyses logs from Azure and AWS you will also be entitled to extensive inventory reporting of those environments.

ESM provides monitoring for regulatory compliance, security best practices, and business policy compliance requirements. To cater for different client requirements, we offer two service variants of ESM - Standard and Enhanced.

Both service variants include monitoring of regulatory compliance and security best practices, however only the Enhanced Service comes with the ability to add customized business policy compliance rules. Notifications will be sent as defined below:

- **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 a pre-defined baseline of NTT'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.

The Enterprise Security Monitoring Service provides:

- 24/7 service desk
- Configurable reporting
- Extensive inventory reporting of your Cloud environments (AWS and Azure)
- Support for custom business use cases (Enhanced)
- Client notifications of security incidents via email (ESM - Enhanced Clients have the option of being notified by an analyst)
- Client access to 90 days of event data

Key Benefits

- Safeguard your business by gaining visibility into activity across your IT infrastructure by bringing all your separate compliance, security best practices, and business policy compliance security controls into one pane of glass.
- Enhanced risk management through effective incident escalation of compliance, security best practices, and business policy compliance violations across on-premise, cloud and hybrid environments.
- Improved agility by freeing up your internal resources to focus on your core business outcomes and requirements.
- Certified SOC environments to protect your data: ISO/IEC 27001:2017, SOC2 Type 1, ASIO-T4 (Australia).

1.2. Service Matrix

The Enterprise Security Monitoring Services are available in two distinct service packages called service variants.

The selected service variant forms part of your *Managed Services Agreement*.

Service Features	Service Variant	
	Standard	Enhanced
Core Service Features		
• Hours of Operation (24/7) • Security Operations Centres (SOCs) • Client Portal • Language Support • Security Appliance	✓	✓
Enterprise Security Monitoring Service Features		
Service Portal and Reporting		
Manage Centre Portal	✓	✓
Client Access to 90 days of Event Data	✓	✓
Configurable Reporting	✓	✓
Cloud Reporting (AWS and Azure)	✓	✓
Detection Types		
Security Best Practices and Basic Compliance Profile	✓	✓
Enhanced Compliance Profile		✓
Custom Business Policy Compliance Rule Creation		✓

Service Features	Service Variant	
	Standard	Enhanced
Customized Event Detection		✓
Security Analyst Interaction		
Automated Event Analysis	✓	✓
Client Notification		
Automated Email Notifications	✓	✓
24/7 Security Analyst Telephone Notifications (High Severity)		✓
Service Options		
Investigator – Enriched and Aggregated Log Search		✓
Secure Long-Term Log Storage (SLTLS)	✓	✓
Advanced Cloud Compliance Reporting		✓
Service Management		
24/7 Service Desk	✓	✓
Service Level Management	✓	✓
Service Delivery Manager	✓	✓
Technical Account Manager (optional)	✓	✓
Service Transition		
Client Transition	✓	✓

Table 1 Service Matrix

1.3. NTT's Managed Security Services Portfolio

Figure 1 MSS Service Menu

2. Core Service Feature Descriptions

2.1. Hours of Operation

Enterprise Security Monitoring Services are delivered through our Security Operation Centers (SOCs), which operate 24 hours a day, 7 days a week.

2.2. Security Operations Centers (SOCs)

We will deliver Enterprise Security Monitoring 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. The Client portal is described in 3.1.1 Manage Centre Portal.

2.4. Language Support

Enterprise Security Monitoring 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 to 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. 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 log feeds from your in-scope devices and systems, then prepares 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 (recommended) form factors
- Security Appliances run a hardened Linux operating system, fully maintained by us
- Log and data capture with compression and secure forwarding to the NTT data center
- Encrypted connections to and from the NTT data center (zero touch ‘phone home’ VPN)
- Custom developed networking to address multi-tenant address space issues
- Provides secure access for backup and restore of your devices under management
- Health and availability monitoring of your devices under management
- Centralized management and configuration

The Security Appliance requires:

- two static (non-dynamic) IP addresses
- permanent LAN Connectivity, and
- 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, and
- 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 LTA 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 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:

- 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 7 – Manage Centre Dashboards and Reports

3.1.2 Security Tools

- For Enterprise Security Monitoring you are provided with a set of Manage Centre security tools for configurable reporting and real time investigational purposes including:
  - Security Event List Viewer
  - Security Event List Dashboard
  - Configurable Reporting
  - Cloud Reporting

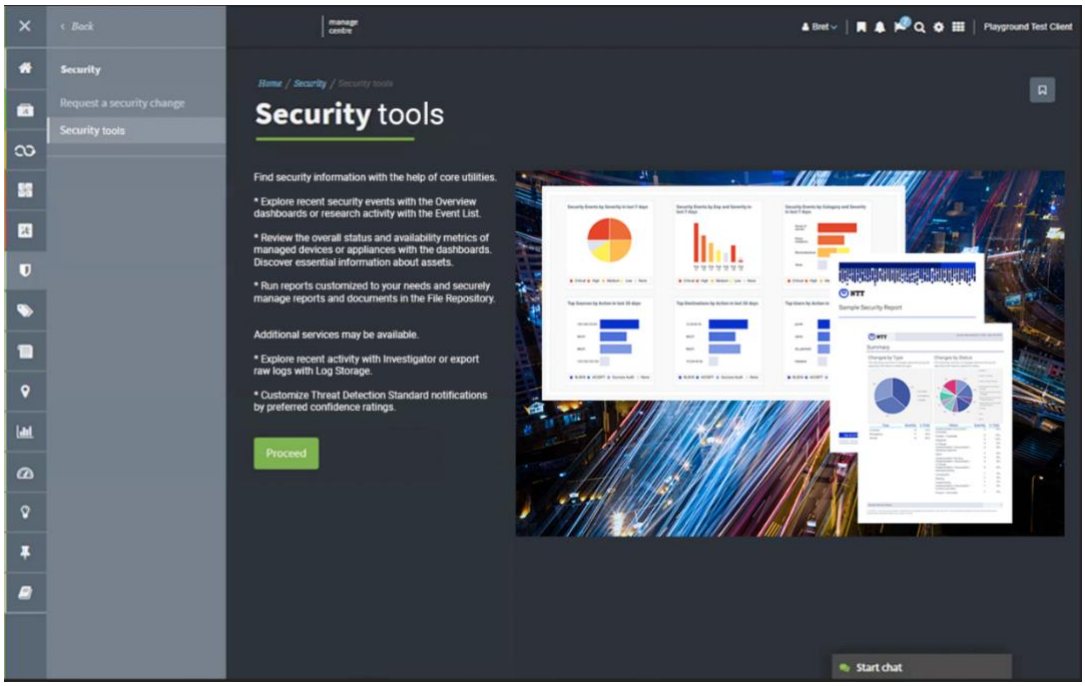

Figure 6 - Manage Centre Security tools

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

- Investigator - an enriched and aggregated log search tool
- Advanced Cloud Compliance Reporting (PRISMA cloud)
- Secure Long Term Log Storage (RAW log storage)

These options are described in 3.4 Service Options.

3.1.2.1 Security Event List and Dashboard

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

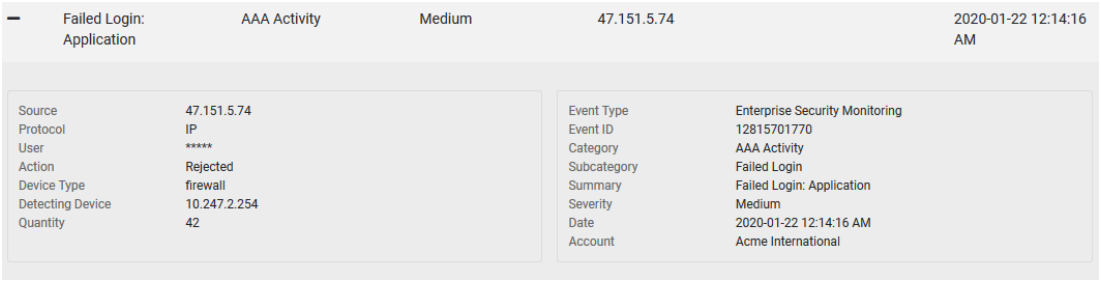

Figure 2 Enterprise Security Monitoring Event List Sample

You also have access to the Security Monitoring 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

3.1.2.2 Configurable Reporting

You will have access to configurable security event reporting, including logs related to security events. Reports can be scheduled or run as needed.

3.1.2.3 Cloud Reporting

If you are subscribed to the log sources in the Supported Device List (Amazon Web Services, Microsoft Azure), you will be entitled to the cloud specific reporting.

We use the Cloud State Scanner (CSS) to gather information in your cloud environment. The CSS is an application which runs in your Kubernetes Namespace in NTT. Only one instance of the application per Client Namespace is required.

Cloud Security Overview Report

The Cloud Security Overview Report provides a current status of the following objects:

- Accounts
- Storage Configuration
- Computing Configuration
- Groups
- Group Configuration

- Users
- User Configuration

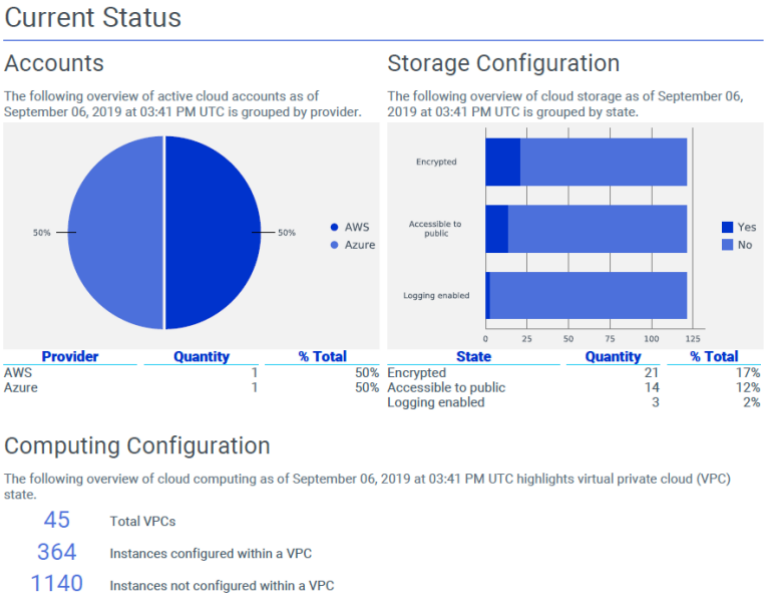

Figure 3 Report Overview - Accounts and Storage

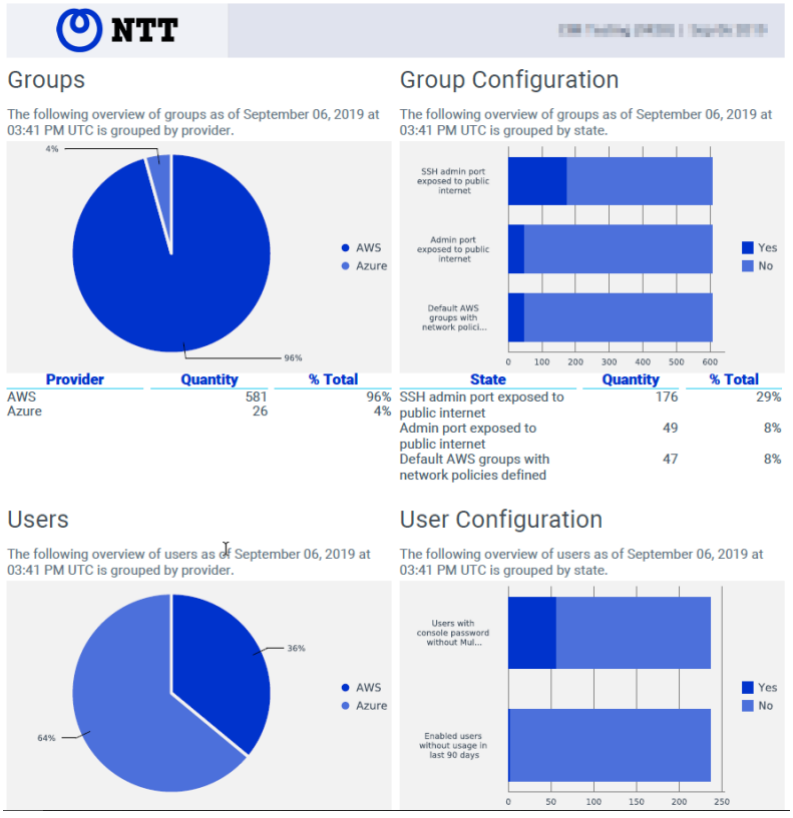

Figure 4 Report Overview - Groups and Users

Trending

The following chart depicts the trend in the objects below. This may provide usefulness to identify security posture over time, indicating an endemic problem or other use cases.

- Storage by Configuration Metric (example below)
- Computing by Total VPCs / VNET
- Groups by Configuration Metric
- Users by Configuration Metric

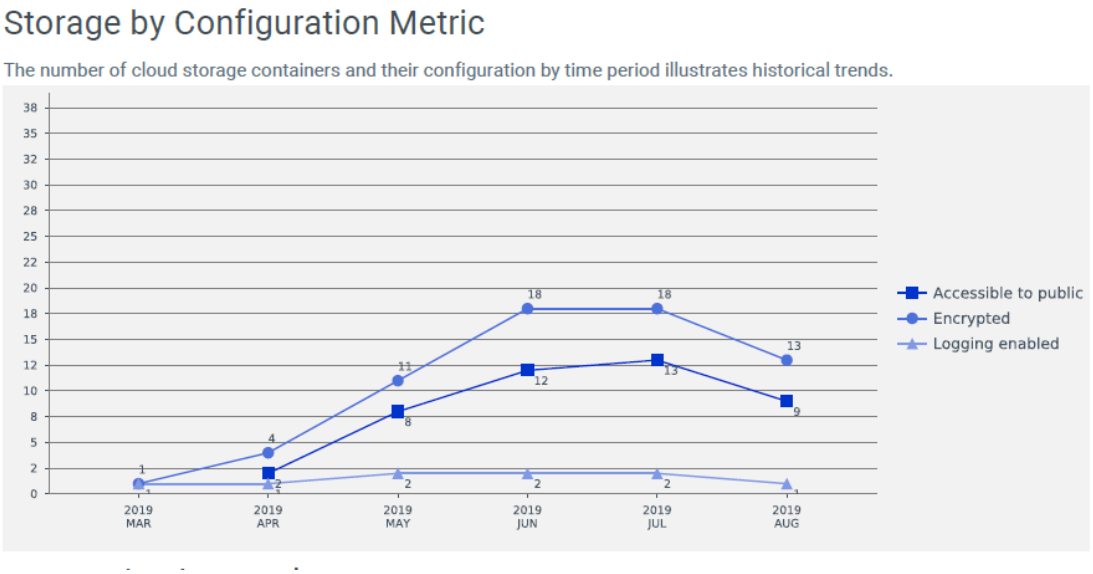

Figure 5 Report Overview - Trending (Storage configuration)

Cloud Security Inventory

The Cloud Security Inventory provides an up to date Microsoft XLS file containing a full list of:

- Storage
- Computing
- Groups
- Users

Asset Type	Fields
Storage	• Account • Provider • Name • Accessible to Public

	• Encrypted • Logging Enabled • Last Seen
Computing	• Account • Provider • Name • Type • VPC/Vnet • Last Seen
Groups	• Account • Provider • Name • VPC • Admin port exposed to Internet • Default AWS/Azure network policies • SSH Admin port exposed to Internet • Last Seen
Users	• Account • Provider • Name • Enabled user without usage in last 90 days • Users with console password without MFA enabled • Last Seen

Table 2 Cloud Security Inventory

3.2. Enterprise Security Monitoring Standard

Enterprise Security Monitoring Standard provides enterprise security compliance monitoring. The level of compliance has been designed for organizations with standardized security detection and compliance requirements across a core set of security technologies.

The following sections discuss the features of the Enterprise Security Monitoring Standard service variant.

3.2.1 Detection Type

Enterprise Security Monitoring Standard uses a standardized security and compliance profile to identify and report on the following categories of security incidents:

- **Compliance** - Events that indicate a deviation from a pre-defined baseline of a regulatory body's definition of compliance controls.
  - PCI-DSS

- HIPPA

- **Security Best Practices** - Events that indicate a deviation from a pre-defined baseline of our definition of security best practices.

Our standard rule sets for existing supported device types are included in the Standard service variant.

To ensure service quality, we will continuously make detection tuning decisions based on the validity and relevance of service generated events and security incidents.

Enterprise Security Monitoring Standard does not include custom business use cases. Implementation of custom business compliance use cases are available in the Enterprise Security Monitoring Enhanced Service. Refer to *3.3 Enterprise Security Monitoring Enhanced* for details.

3.2.2 Security Analyst Interaction

Enterprise Security Monitoring Standard utilises automated detection for high confidence security incidents.

3.2.3 Client Notification

Enterprise Security Monitoring Standard uses automated notifications. You will be notified via e-mail and can view events and security incidents on the Manage Centre Portal.

3.3. Enterprise Security Monitoring Enhanced

The Enterprise Security Monitoring Enhanced service variant has been designed for organizations with custom security detection and compliance requirements across a wide set of security technologies.

The following sections discuss the features of the Enhanced service variant.

3.3.1 Detection Type

Enterprise Security Monitoring Enhanced uses customized security detection and compliance profiles to identify and report on the following categories of security incidents:

- **Compliance** - Events that indicate a deviation from a pre-defined baseline of a regulatory body's definition of compliance controls.
  - PCI-DSS
  - HIPPA
- **Security Best Practices** - Events that indicate a deviation from a pre-defined baseline of our definition of security best practices.

- **Business Policy Compliance** - Events that indicate a deviation from a pre-defined baseline of an organization's custom business policy compliance requirements.

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 our standard rule sets for existing supported device types is included in the Enhanced Service variant.

3.3.2 Custom Business Policy Compliance Rules

For Enterprise Security Monitoring Enhanced, additional custom use cases can be created. Enterprise Security Monitoring Enhanced includes a predefined number of rules of variable complexity. Additional rules can be purchased via the Move Add Change Delete (MACD) process as described below.

- **Included in the service**: Up to 15 Standard[1] or Compound[2] Rules can be developed and implemented annually for Enhanced Service clients.
  - Additional Standard or Compound Rules can be purchased via the MACD process at a rate of 6 MACDs per rule.
- **Included in the service**: Up to five (5) existing Analyzers[3] can be implemented annually for Enhanced Service clients.
  - Additional existing Analyzers can be purchased via the MACD process at a rate of 12 MACDs per Analyzer.
  - Development of new Analyzers 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.

3.3.3 Security Analyst Interaction

Enterprise Security Monitoring Enhanced Service utilises automated detection for high confidence security incidents.

3.3.4 Client Notification

A combination of automated and manually created notifications are utilized for Enterprise Security Monitoring Enhanced. You are notified based on your selection

[1] An ESM detection method that tests a single attribute within a single log line to generate an Event (e.g. if a specific message number is identified, then an Event should be generated).

[2] An ESM detection type that tests multiple attributes within a single log line to generate an Event (e.g. if a specific user logs into a specific server, then an Event should be generated).

[3] An ESM detection mechanism that requires detailed analysis and development. (e.g. A detection mechanism which triggers an event if a user is created and added to a privileged group in the configured duration, scoped on username).

of supported notification options, including e-mail and phone calls (for high severity events).

3.4. Service Options

3.4.1 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, Investigator also archives a copy of logs in a secure, cloud-based repository. Online access to enriched and aggregated logs through the Manage Center 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.

Enterprise Security Monitoring 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 Center Portal.

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

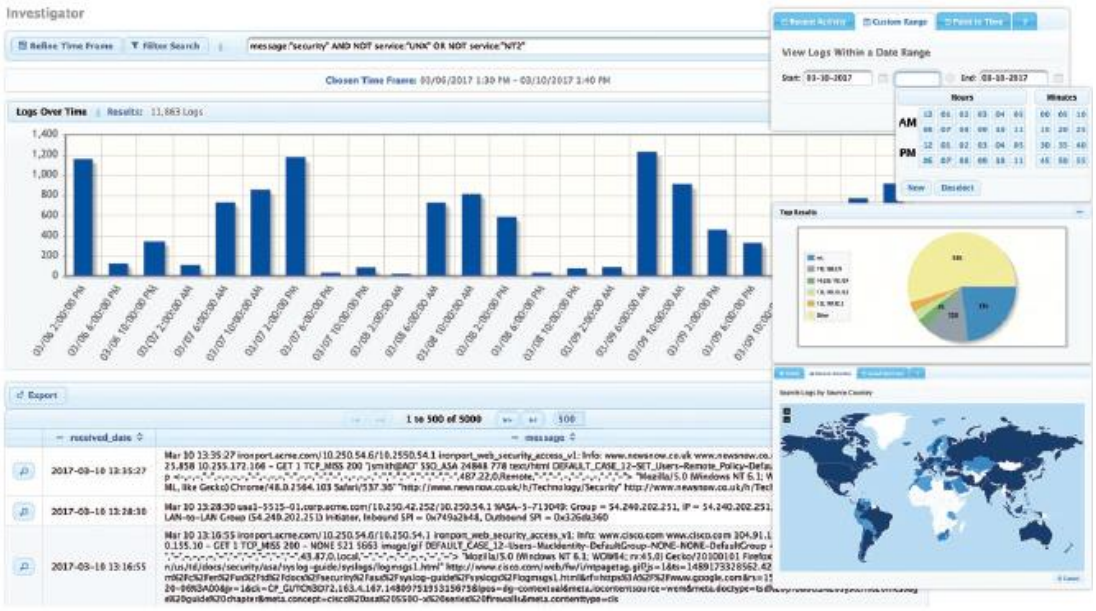

Figure 6 Investigator

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 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 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.

3.4.2 Secure Long-Term Log Storage (Optional)

The Secure Long-term Log Storage (SLTLS) option is available for both Enterprise Security Monitoring Standard and Enhanced clients.

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 services. SLTLS is not customizable to specific devices or IP addresses.

The SLTLS option utilizes proprietary data storage software to securely store raw logs in originally obtained unaltered format. The SLTLS option 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 a basic log search based on date/time parameter and a single IP address, resulting in a list of compressed raw log files matching the parameters, which you may download locally for further investigation on your local computer.

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.

3.4.3 Advanced Cloud Compliance Reporting

Enterprise Security Monitoring Enhanced clients with a Prisma Cloud subscription have the option to enable Advanced Cloud Compliance Reporting. This feature provides you with integrated data reporting in the Manage Centre portal.

Reports can be scheduled or on demand. When scheduled, the reports will be available for download from within the Manage Centre Portal.

Supporting both AWS and Azure, relevant compliance reports include:

- CIS
- NIST
- PCI DSS
- HIPAA
- GDPR

- ISO
- SOC 2
- HITRUST

You will be required to authorize read only access to NTT to retrieve events from your cloud for the purpose of report generation.

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 organisation 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, or
- directly reported by 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 MSS Technical Account Manager (Optional).

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 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, 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 NTT 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 NTT's 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 the NTT MSS delivery model who 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. Clients benefit from the MSS Technical Account Manager Team support of internal and external stakeholder management while they face challenges implementing security controls across their 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 for clients 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 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. 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.

Appendix A Service Level Agreements

Category	Description	Priority	SLA	Service Credits	Service Credit Limit
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	N/A	N/A
		P3 and 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
		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 mins	N/A	N/A

Appendix B