Client Service Description

Security Operations Centre as a Service (SOCaaS)

19 January 2021 | Document Version 1.3

NTT contact details

We welcome any enquiries regarding this document, its content, structure, or scope. Please contact the MSS Product Office, or your local representative.

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 *SOCaaS – Client Service Description* in any correspondence or order.

Confidentiality

Terms and conditions

Document Preparation

	Name	Title	Date
Prepared:	Tore Terjesen	Product Manager - Security Division	19 Jan 2021

Release

Version	Date Release	Pages	Remarks
1.0	30 Oct 2020	All	Final version

Version	Date Release	Pages	Remarks
1.1	05 Nov 2020	25	Removed Figure 3 for NTT Threat Intelligence
1.2	20 Nov 2020		SLA Added
1.3	19 Jan 2021	19	Added Information Security Engineer (ISE) description
		23	Updated CTS description. From SOC analysis of events to automated Security Incident reports
		46	Updated MACD table in Appendix A
		49	Added Service Governance table in Appendix C

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.

Contents

List of Figures

List of Tables

1 Service Overview

Organizations across the globe are battling an ever-evolving threat landscape while juggling growing costs and security complexity. Analytics-driven Security Information and Event Management (SIEM) platforms are a fundamental element to an organization's security strategy to manage these challenges. However, the platforms alone don't bring about the transformation needed to achieve the primary goals. Timely detection of threats and compliance violations and the ability to manage incidents with minimal impact are paramount to many organizations facing constant threats and budget constraints. Mature and progressive operations need to factor business context, expertise, processes and procedures to optimize 24/7 security monitoring and incident management efficacy and expense.

NTT's SOC (Security Operation Centre) as a Service offers tailored services to transform your security operations. We will proactively manage, maintain and monitor your SIEM platform and augment its threat visibility with NTT's advanced network traffic analysis (NTA). Delivered by certified SIEM engineers and experienced analysts from our 24/7 SOCs, we establish a consolidation point that provides real-time visibility of your environment helping you to manage risks, detect advanced cyber-attacks, support complex compliance requirements and control costs.

Detection, analysis and detailed security incident reporting of cyber-attacks are delivered through a combination of NTT tools and market leading SIEM platforms. NTT's network traffic analysis technology is added to give greater insight into the detection of cyber threats. Events are investigated and validated by Security Analysts following well-defined escalation processes to ensure that you receive reliable and accurate incident reports in a timely manner allowing for an informed and actionable response.

Compliance monitoring and reporting are delivered using the native capabilities of the SIEM platform. We will install and configure applicable compliance framework rules sets, dashboards and reports. Adherence to business policy compliance can be achieved with custom use cases according to your requirements.

SOC as a Service supports market-leading SIEM platforms. If you don't already have a supported SIEM platform, we can either migrate your existing deployment or build a new environment utilizing our best-practice installation and configuration guides.

SOC as a Service provides:

- SIEM platform management including health and availability monitoring, software patching, OS maintenance, backup and restore
- SIEM platform configuration including fine-tuning of rules, creation of custom use-cases, dashboards, reports and log parsers
- 24/7 monitoring of events and alerting of security incidents based on investigation and validation by SOC analysts
- Enhanced threat visibility leveraging NTT's Cyber Threat Sensor providing advanced network traffic analysis, machine learning and threat intelligence
- Compliance monitoring, reporting and notification based on client requirements
- Certified SIEM engineers and SOC analysts

The benefits include:

- Improved security stance with continual reduction in business risks, administrative burden, and costs
- Strengthened security posture by analysing cyber threat activity directly on the network that may evade SIEM rules, blind spots or standard security controls
- Improved audit process, alignment and ability to satisfy regulatory or industry compliance requirements and objectives
- Optimized return on existing capital investment in your SIEM platform
- Portable solution since you own the SIEM platform and everything that NTT builds within it
- Maximized functional use of the SIEM platform aligned to your business requirements
- Scalable and flexible SIEM operations according to your current needs
- Transferred SIEM operational tasks allowing client teams to focus on strategic initiatives

2 Service Matrix

Managed Security Services are available in packages consisting of a core set of Service Modules, associated service Elements and options. This document presents Security Operation Centre as a Service (SOCaaS).

Service Elements	Included
Core Service Elements	
Hours of Operation (24/7)	✓
Security Operations Centres (SOCs)	✓
Client Portal	✓
Communications	✓
Escalation Management	✓
Service Transition	
Inception	✓
Definition	✓
Build	✓
Deployment	✓
Close	✓
Service Content	
Client Notification	
Analyst-created Security Incident Reports Based on Detailed Investigation	✓
Cyber Threat Sensor automated Security Incident Reports	✓
Portals and Reporting	
Client Portal – Security Incident tickets	✓
SIEM User Interface for Compliance Reporting and Dashboards	✓
Compliance	
Customized Monitoring	✓
Customized Reporting	✓
Customized Dashboards	✓

Service Elements	Included
Detection of Cyber Threats	
Detection Capabilities	
NTT's Cyber Threat Sensor	✓
Threat-related Detection Capabilities within the SIEM Environment	✓
Detailed Security Incident Investigation by Security Analyst	✓
SIEM Platform Management	
Health and Availability Monitoring	✓
Incident Management	✓
Capacity Management	✓
Configuration Management	✓
Service Request Fulfilment	✓
Service Management	
Information Security Engineer (ISE)	✓
Service Delivery Manager	✓
Technical Account Management (Optional)	✓

Table 1 Service matrix

3 NTT's Managed Security Services Portfolio

Figure 3 MSS Service Menu

4 Core Service Elements

4.1 Hours of Operations

Managed Security Services are delivered through NTT's Security Operations Centres (SOCs). Unless otherwise stated, MSS hours of operation are 24 hours a day, 7 days a week.

4.2 Security Operations Centres (SOCs)

NTT shall deliver services through any of their SOCs, at the sole discretion of NTT. Client data may be held in any SOC and/or NTT's infrastructures unless there is prior agreement and approval between NTT and the Client.

4.3 Client Portals

For the SOCaaS offering, you have access to the following portals:

- Client portal
- Native SIEM user interface (UI)

4.3.1 Client Portal

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

4.3.2 SIEM UI

Clients access the local SIEM-system where the native capabilities of the in scope SIEM-system are used to present compliance related reports and dashboards included in the service. The SIEM UI is available to you for all types of investigations.

4.4 Language Support

SOCaaS is provided in the English language only, unless there is prior agreement and approval between NTT and you.

4.5 Co-Management

In addition to the native access to the SIEM UI, as necessary and required by you, NTT will allow you to create and run client-designed reports and queries.

Any privileged activity in the SIEM UI must be coordinated and agreed with NTT ahead of time by raising a Service Request.

Any outages incurred due to client behavior will be considered outside of recorded service levels and will be tracked separately for governance reporting purposes.

4.6 Security Appliance

Most SOCaaS solutions require an NTT Security Appliance, including SaaS based SIEMs as they may require on-premise log forwarding components. The Security Appliance is used for Health and Availability monitoring and as a proxy for management of the SIEM configuration items and the Cyber Threat Sensor

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.

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
- 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
- centralized management and configuration.

The Security Appliance requires:

- One or two non-dynamic IP addresses (depending on the environment)
- Permanent LAN connectivity
- Permanent Internet connectivity to NTT infrastructure 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

4.7 Communications

4.7.1 MSS Infrastructure

NTT utilizes a regional-based infrastructure with built-in security by design principles. It is highly resilient, secure, and uses best-practice methodologies, tools, and techniques.

4.7.2 Notifications

4.7.2.1 Email

For security and data privacy reasons, email notifications will only contain minimal information to notify you about the creation of, or updates to, tickets.

You may send emails relating to new or existing tickets to NTT. In the case where no reference number is provided as formatted by us, NTT shall create a ticket with a short description based on the subject line provided.

When you are replying to an email with an existing reference number (as provided by NTT and unchanged by you), the message body text shall be copied (upon receipt) to the journal of the relevant ticket, and shall be marked as updated by you and waiting on NTT's further input. For security reasons, if you wish to send sensitive information to us or provide approval workflow pertaining to an existing or new ticket, you are urged to do so using the client portal.

4.7.2.2 File attachments

Diagrams, images, PDFs, executables, and any other attachments must not be attached to any case via email. Where file attachments are necessary, you must log into the client portal and attach the file securely through your web browser connected to the client portal.

4.7.2.3 Telephone

NTT's SOC staff may contact you, and you may contact the NTT Service Desk by telephone. In both cases, an authentication shall be completed to verify your identity.

4.7.2.4 Client Portal

Unless otherwise stated and agreed, all other communications originating from the SOCs shall be secure, follow security best practices, and shall be available via Manage Centre.

4.7.3 ITSM (Service Management)

NTT's ITSM system manages tickets aligned with ITIL, wherever appropriate. Only appropriate NTT staff have access to the ITSM tool.

4.7.4 Connection to Client Network

You must supply all the necessary network hardware and cabling to connect the configuration item to your own, third party and ISP networks. All network interfaces connecting to the configuration items must be a minimum of one gigabit Ethernet interfaces. The standard for gigabit stipulates auto mode as mandatory. However, some manufacturers have deviated from this and do facilitate the hard coding of interface speed and duplex. Where this is enabled, it is imperative that both ends of the network cable are set to fixed speeds and duplex modes (in other words, both switch and configuration item). In this instance, it is important that you discuss any potential infrastructure changes that may affect this setting during service transition or directly with the SOC during service operation.

4.7.5 Engineering

4.7.5.1 Configuration Item Access

Command-line access to management consoles within your premises are secured using SSH v2 from NTT jump hosts leveraging the Virtual Private Network (VPN) established from the Security Appliance. For third party supported SaaS applications this is not applicable.

4.7.5.2 Application Access

Application-specific protocols to access management consoles within your premises are secured using SSH v2 and HTTPS from NTT jump hosts leveraging the VPN established from the Security Appliance. Third party SaaS applications are accessed via the public Internet leveraging the vendors chosen security protocols.

5 Service Transition

Service transition is executed in five phases:

1. Inception
2. Definition
3. Build
4. Deployment
5. Close

The five phases and their corresponding activities and procedures ensure a consistent approach to management and completion of the transition and a framework for governance and communication. During the first four phases of the service transition period, no alerts, incidents, or cases will be generated for your review and triage.

The activities in each phase below are defined for a greenfield deployment. When NTT takes on the responsibility of an existing SIEM environment, these activities are modified accordingly.

5.1 Inception Phase

To initiate the service transition, you submit a Purchase Order (PO) along with the pricing information from the approved quotation, and the Transition Workbook.

NTT reviews the documentation provided by you and confirms that all the requirements for commencement of the transition have been met.

A kick-off meeting is held to communicate the transition process, project tasks, roles and responsibilities, and introduce the key stakeholders.

The Inception Phase is expected to take 12 business days and can be accelerated if you provide complete and accurate documentation when submitting the Transition Service Request.

5.1.1 Inception Phase Activities

The key activities during the Inception Phase are:

- Receive the Service Transition Request containing a complete copy of the executed client contract, the High-Level Solution Design (HLSD) document, the Transition Workbook, PO and any approved non-standard requests (NSTARs)
- Review the documentation provided to confirm the content is complete and aligned and either accept or reject (with feedback) the Service Transition Request within 3 business days
- Assign a Service Transition team, including the identification of NTT's Service Delivery Manager.
- Initiate request for Security Appliance(s) (physical or virtual)
- Initiate request for Cyber Threat Sensor(s)
- Schedule and conduct a kick-off meeting
- Configure client portal account(s)
- Configure client entitlement(s) in NTT's ITSM

5.1.2 Inception Phase Deliverables

The deliverables provided during the Inception Phase are:

- Schedule and conduct the Kick-off meeting (face-to-face or call) and presentation
- Shipment of CTS, Security Appliance and SIEM software / hardware

5.2 Definition Phase

During the Definition Phase, NTT validates connectivity with the client-installed hardware/software shipped during Inception and finalizes the Project Schedule with you. The Planning Phase is expected to take 15 business days.

5.2.1 Definition Phase Activities

The key activities during the Definition Phase are:

- Client confirms receipt of the shipped software / hardware
- Client installs the software / hardware
- NTT confirms connectivity to the client-installed software / hardware
- NTT and the Client finalize a mutually agreed Project Schedule
- Review, update and agree on architecture and in-scope log sources
- Assess log source scope and prioritization, including completing the Log Source Inventory, where applicable.

5.2.2 Definitions Phase Deliverables

- The final Service Transition Project Schedule.

5.3 Build Phase

The Build Phase establishes the primary service elements for NTT to provide MSS. It includes connectivity, appliances for log collection and SIEM Platform management access, and client portal and ITSM setup. The Build Phase is expected to take 20 business days.

5.3.1 Build Phase Activities

The key activities during the Build Phase are:

- SIEM environment equipment installation and deployment
- Setup and validation of remote access
- Out-of-band (OOB) management configuration (if applicable)

5.3.2 Build Phase Deliverables

The deliverables provided during the Build Phase are as follows:

- SIEM environment built, implemented, operational, and accessible
- Test results

5.4 Deployment Phase

The Deployment Phase completes the technical service elements required by NTT to provide the service. It includes configuration of all purchased services - log source onboarding and log collection, rules and use case creation and implementation, reports and dashboards creation, tuning and normalization, finalization of solution documentation, and final client portal and ITSM integration. Additionally, NTT will conduct a SOC synchronization meeting and client portal training, just prior to go live, with you. The Deployment Phase is expected to take 45 business days.

Following the SOC synchronization meeting, the Service Delivery Manager and the Information Security Engineer (ISE) become the interface into NTT services.

5.4.1 Deployment Phase Activities

The key activities during the Deployment Phase are:

- Device(s) onboarding, log(s) ingestion, service testing, and final verification
- Normalization and tuning (logs/use cases)
- Quality assurance review and activation of the service(s)
- Final validation of connectivity to the SOC
- Risk and issue documentation
- MSS SOC synchronization meeting with the Client
- MSS SOC client portal training meeting with the Client
- Confirm Service Activation Date (in phases, if required), billing date, and SLA start date

5.4.2 Deployment Phase Deliverables

The deliverables provided during the Deployment Phase are:

- SOC synchronization meeting and client portal training
- Service Activation Date
- Confirmation of SIEM platform management readiness
- Client review and acceptance of the Risk and Issue Register
- Final solution architecture
- Incident Alerting Handbook
- Technical Solution Guide

5.5 Close Phase

The Close Phase confirms that the service is live, all deliverables have been produced, and all success criteria has been accomplished to close the Service Transition Project. The Close Phase is expected to take 6 business days.

5.5.1 Close Phase Activities

The key activities during the Close Phase are:

- Conduct Service Transition Plan closure review meeting with the Client
- Review all remaining open action items including lessons and risks/issues to be considered for Steady-State Governance (going forward)
- Receive Client agreement to close the project

5.5.2 Close Phase Deliverables

The deliverables provided during the Close Phase are:

- Risks, Actions, Issues, Decisions (RAID) Log (if any)
- Commencement of service and billing
- Project closure presentation, to include lessons learnt (if any)

5.6 Service Transition Deliverable Acceptance

The service transition is considered complete on the Service Activation Date and after any Close Phase deliverables are provided. The deliverables are considered as being accepted at the completion of the next phase. The Client will close the service transition project by agreeing to the closure of the parent ticket in the NTT ITSM system.

6 Service Features

6.1 Information Security Engineer

The NTT Information Security Engineer (ISE) provides technical expertise in relation to your SIEM solution. An ISE is assigned during the service transition and will act as your trusted advisor and technical liaison as well as the Service Delivery Manager. It is the task of the ISE to understand your unique environment, business vertical, log sources, use cases, and compliance needs.

Deliverables of the ISE include:

- Weekly, monthly, and quarterly technical calls
- New use case suggestions and implementation based on your environment and need
- Use case tuning and updates
- Creation and updating of new dashboards
- Creation and updating of new reports
- Working directly with the vendor for troubleshooting, when applicable
- New log source onboarding and validation
- Supplemental log investigations in relation to potentially undetected threats

Advisory and design related to use cases, dashboards and reports or other custom requests are included in the Service. Implementation will incur deduction of Move, Add, Create, Delete (MACD) service units.

Please refer to Service Appendix C for an overview of the technical meetings and participants list.

6.2 Service Portal and Reporting

The Manage Centre Portal (Manage Centre) is the main portal for service requests, change requests, incidents, security incidents and ticket level reporting while compliance reporting, dashboards and event information is available in the SIEM.

When the SOC creates a Security Incident Report, a corresponding ticket is created in Manage Centre and an email notification is sent to you. You can conduct further investigations by using your SIEM tools.

6.2.1 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
- 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, you 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 4 Manage Centre Dashboards and Reports

6.2.2 Security Tools

For SOCaaS you can access security tools and view health and availability information of the configurations items under management.

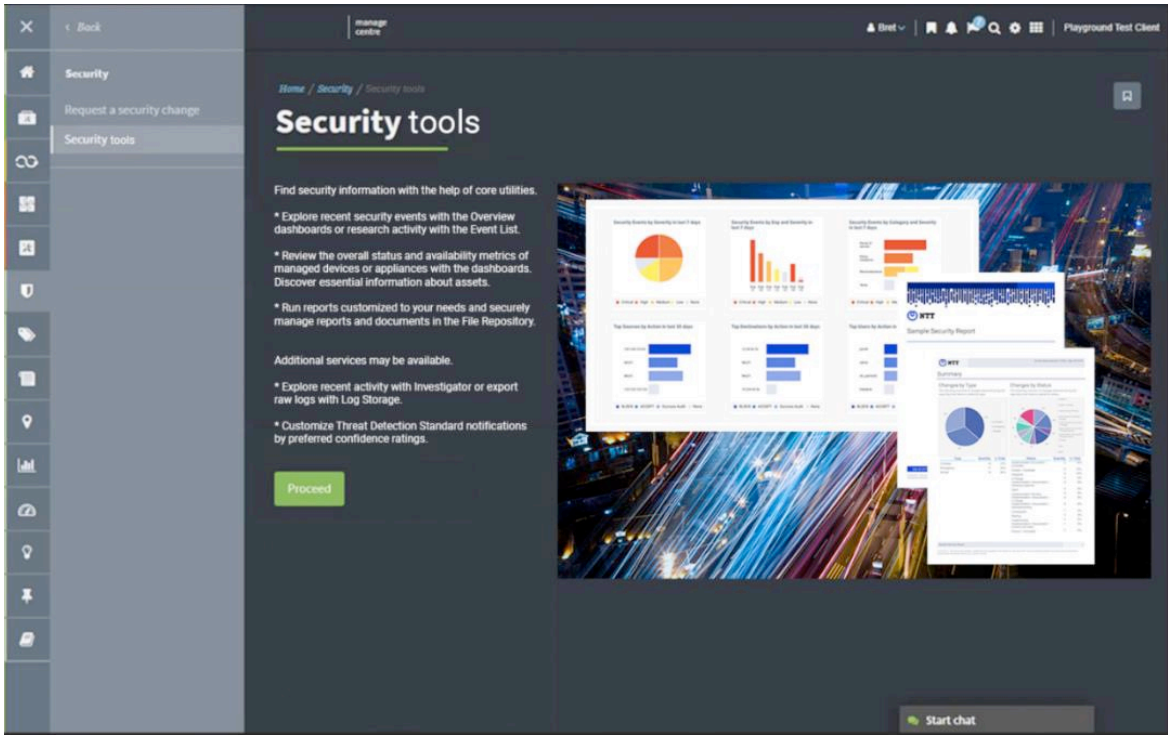

Figure 5 Manage Centre Security tools

6.3 Client Notification

As the SOC identifies security incidents, Security Incident Reports are created.

The reports include a detailed description of the threat, identified activity, impact, and a recommendation of suitable incident response steps to take by you. NTT will notify you based on your selection of NTT's supported notification options.

Notification option availability:

- **Critical severity**; Phone call and 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 to Manage Centre for details.

Note. It is your responsibility to take corrective actions. NTT is only responsible for providing the alert (unless Device Management is in scope of the contract).

Phone call notification details

Clients with phone call notifications must provide NTT with a prioritized list of client contacts. This list may contain three or less client contacts with phone notifications selected.

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

If NTT is unable to reach a contact, NTT will leave a voicemail and move on to the next contact.

6.4 Compliance Monitoring, Notification and Reporting

6.4.1 Overview

Being able to adhere to compliance frameworks and pass audits requires the ability to put forward solid reporting in order to prove adherence to controls. SOCaaS leverages the compliance reporting capabilities of market leading SIEM systems with a broad support for compliance frameworks, be it regulatory or industry compliance.

6.4.2 Compliance Monitoring

As part of the deployment project of a new SIEM or assessment of an existing SIEM, we will install and configure client requested compliance packages (PCI, HIPAA, SOX, etc.) available from the SIEM vendor. This includes configuration of dashboards and reporting in the SIEM UI. Once service transition is complete and the service is live, NTT will install compliance package content updates from the SIEM vendor as part of service delivery. Implementation of Client requested changes to existing dashboards and reports or any other customization is administered through Service Requests and the Move, Add, Change, Delete (MACD) service unit model as defined in *Appendix A*.

6.4.3 Custom use case development

NTT will develop and deploy custom use cases as required by you. Implementation of custom use cases on the SIEM is managed through the Move, Add, Change, Delete (MACD) service unit model as defined in *Appendix A*

6.5 Detection of Cyber threats

6.5.1 Introduction

Cyber threat rule packages are installed and maintained on the SIEM as per your requirements. SIEM threat events are investigated by the SOC and Security Incident Reports are made available on Manage Centre.

While the SIEM environment is the heart of the service, NTT also brings to bear our proprietary network traffic analyser, the Cyber Threat Sensor (CTS).

Our Security Analysts also use the industry aligned MITRE ATT&CK Framework as guidance in understanding and assigning severity to identified security incidents.

6.5.2 SIEM Threat Detection

NTT will install and maintain native SIEM threat detection rule sets. Signature content updates are installed nightly as they are made available by the SIEM vendor. Threat events will be sent to the SOC for further analysis. NTT will proactively tune rules in order to avoid flooding of false positives events. Tuning of rules is included in the service. When tuning rules, NTT will open a ticket in order to create a proper audit trail of changes to the system.

6.5.2.1 Vulnerability Correlation

SOCaaS Clients that have vulnerability scanners or vulnerability scanning capability within their environment will be able to ingest that vulnerability data into the SIEM. This capability allows NTT to have increased accuracy in the performance of the analytics function, reduces false positive alerts, and ultimately provides better fidelity of the service overall.

6.5.3 Cyber Threat Sensor

NTT's network traffic analyser, the Cyber Threat Sensor (CTS) is included in the service. The CTS strengthens your security posture by analysing cyber threat activity directly on the network that may evade SIEM rules, blind spots or standard security controls.

The CTS produces automated high confidence security incident reports that include incident information and remediation recommendations.

The CTS is a network traffic analyser, only requiring a TAP or a SPAN port for access to the traffic flow.

SOCaaS includes one Perimeter CTS monitoring the traffic in and out of your perimeter. Additional Perimeter and Internal sensors may be subscribed to as per your requirements and network infrastructure. Internal monitoring points are highly recommended for detection of lateral movement activity.

The sensor is lightweight and easy to install as it is delivered as software with a small footprint. The CTS is installed by you according to NTT's requirements. You are responsible for underlying hardware or virtual infrastructure to house the CTS. The following table provides an overview of the capabilities:

Cyber Threat Sensor Capabilities
Threat detection capabilities
Advanced Analytics (machine learning / behavioural modelling) on Network Layer
Threat Reputation and Pattern Signature Matching on Network Layer
Cross Device Correlation (lateral movement)[1]

Table 2 Cyber Threat Sensor Capabilities

6.5.3.1 Placement of the CTS

- **CTS Perimeter**
  - One Perimeter CTS is included in the Service
  - Monitors your network perimeters (e.g. internet breakout, DMZ), delivering threat detection monitoring of client traffic towards and from the Internet.
- **CTS Internal**
  - Internal CTS' are optional devices.
  - 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 when your assets are able to connect towards the Internet.

A CTS may monitor multiple VLANs as long as the combined traffic does not exceed 1 Gbps. If the bandwidth exceeds 1 Gbps the load can be split between multiple CTS devices without any quality impact to the service. The traffic can be split by using a TAP/SPAN/Mirroring technology and direct the traffic to different CTSs based on VLAN, IP's and Net ranges.

6.5.3.2 Lateral Movement Detection

Clients subscribing to multiple CTS devices and placing these throughout their network estate benefit from cross device correlation, where the combined insights of all CTS devices are correlated to enable detection of threats moving laterally and to better understand the potential impact.

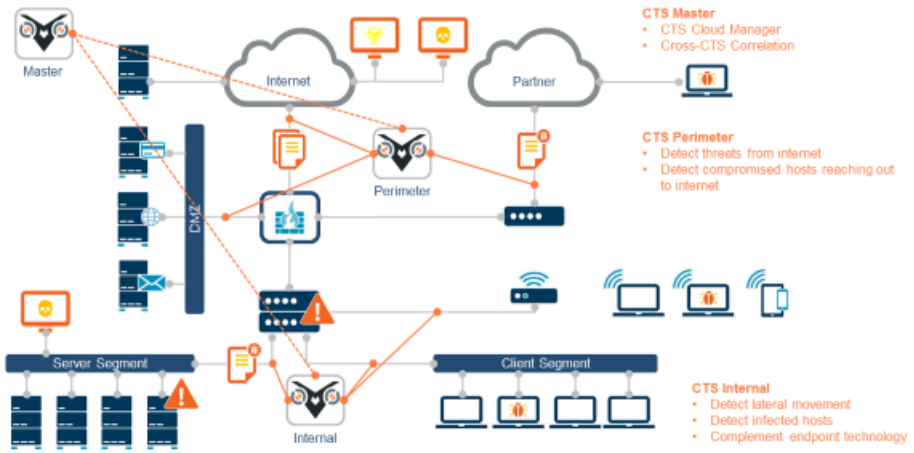

Figure 6 Cyber Threat Sensor placement

As CTS devices identify suspicious activities throughout your network, events (silenced and normal) are sent upstream to the CTS Cloud Manager (hosted in NTT infrastructure) to a Master CTS Threat Detection Analysis Engine, which cross correlates the activity. The combined sum of the suspicious activities is used to identify threats while also providing a deeper understanding of impact and how widespread the threats are.

6.5.3.3 Incorrect Placement of CTS Internal

[1] For Clients subscribing to multiple CTS devices

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 to change the monitored traffic to network type in scope for CTS Internal.

6.5.3.4 CTS Threat Detection Capabilities

The CTS device identifies threats by analysing traffic on your networks using a combination of Advanced Analytics, traditional detection techniques, and Threat Intelligence.

Advanced Analytics

Today's sophisticated threat actors continuously switch between a variety of Tactics, Techniques and Procedures (TTPs) to avoid detection. This have left traditional security measures (e.g. perimeter and endpoint protection), which rely on common detection techniques (e.g. Reputation / Pattern / Correlation) struggling, in the identification of, and response to, these evasive threats.

To efficiently detect these threats one must adopt a security monitoring solution that consists of multiple layers of technologies/sources and detection techniques, then analyse the combination of these using signature-less types of detection techniques, as employed by NTT's Threat Detection Engine.

Threat Intelligence

The CTS leverage curated threat intelligence from NTT and external partners for development of AI/ML detection capabilities, threat reputation and pattern signature matching.

6.5.3.5 Operating System/Software Management

NTT maintains the supported Operating System (OS) and installed software on CTS devices. Such maintenance is performed remotely and at the sole discretion of NTT. Updates are applied as relevant security hotfixes are made available, or as part of standard OS software management.

6.5.3.6 Health and Availability Monitoring

NTT monitors 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 device 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. Upon identifying health and availability related issues which risk NTT's 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

NTT utilizes standard poll cycles and thresholds when monitoring the CTS. NTT may adjust the thresholds based on the historical data collected to eliminate unnecessary events from occurring. With this data, NTT 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 the sole discretion of NTT, outside of any client change management process.

6.6 SIEM Platform Management

6.6.1 Overview

The service includes a 24/7 managed SIEM environment including continuous health and availability monitoring of the SIEM environment, management of the SIEM servers, patch management, and configuration backup and restore of the OS and application

Monitoring of log source health is delivered using the native SIEM capabilities.

6.6.2 Log Source Health Monitoring

NTT will monitor log source health using native SIEM capabilities. If the SIEM reports an issue with a log source, NTT will notify you by automatically creating a ticket or make it available in a dashboard or a report as per your requirements. Associated investigations related to issues with log sources are charged as per the MACD table.

Management of log source devices is not included in the service, however NTT offer device management services for network and security devices, both on premise and in the cloud. Please contact your sales representative for more information.

6.6.3 Health and Availability Monitoring

NTT's Health and Availability (H&A) Monitoring utilizes the MSS infrastructure to provide 24/7 H&A monitoring of the SIEM environment and notifies you of any incidents which may cause disruption to the service.

6.6.3.1 Health and Availability Monitoring

The service includes monitoring of key performance indicators of in-scope configurations items state and resource utilisation to determine the overall health, performance, and availability.

The service automatically generates incidents in the NTT 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. For more information, see *6.6.4 Incident Management*.

You will be notified and kept up-to-date of issues with overall H&A via the incident ticket available on Manage Centre.

6.6.3.2 Health and Availability Improvement and Recommendation

NTT utilises standard poll cycles and thresholds when monitoring in-scope configuration items. NTT may adjust the thresholds based on the historical data collected to eliminate unnecessary events from occurring. With this data, NTT may identify potential methods of improving configuration item performance and overall H&A.

6.6.3.3 Health and Availability Change Implementation

If a configuration item requires changes, NTT shall follow the standard change management process.

6.6.3.4 Third Party Software as a Service (SaaS)

You are responsible for the H&A of your Internet connection and third party services/applications.

Note. NTT is not responsible for H&A of third party SaaS applications.

6.6.4 Incident Management

Incident management is the process for managing the lifecycle of an incident. The aim is to restore the service as quickly as possible to minimize business impact. This is achieved through a temporary workaround or permanent fix, within the service level targets.

As part of the SOCaaS, NTT proactively identifies incidents on configuration items.

6.6.4.1 Incident Generation

Incidents may be generated through H&A Monitoring by the SOC or by you raising an incident via Manage Centre or a telephone call to the service desk.

After an incident case is raised via Manage Centre, with a provided impact and urgency, the SOC team will validate the ticket and reserve the right to modify the impact and urgency, as deemed necessary.

For an incident case raised via a telephone call to the service desk, the service desk shall create an incident case on your behalf with the relevant impact and urgency.

For any urgent service disruption, NTT will advise you to open a case in Manage Centre and follow up with a call to the service desk using the ticket number.

6.6.4.2 Incident Diagnosis

Incident tickets are managed based on the priority of the incident ticket raised in Manage Centre. Priorities are calculated based on the impact and urgency of an incident ticket. Priorities are defined as major, high, moderate, and low.

		Urgency		
		1. Work Blocked	2. Work Degraded	3. Work Not affected
Impact	1. Organisation wide	Major	Major	High
	2. Multiple departments	Major	High	Moderate
	3. Single department	High	Moderate	Low
	4. Individual	Moderate	Low	Low

Table 3 Impact-Urgency matrix

The SOC will triage the incident to assess the priority. Incidents will be assigned to the appropriate SOC engineer for further investigation and analysis to identify a correction plan to resolve the incident. Using Manage Centre, NTT notifies you of updates to an incident and any restoration plan to resolve the ticket.

6.6.4.3 Incident Resolution

NTT shall work 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:

- confirm resolution and the incident will be moved to a closed state
- do not respond, and the incident will be auto closed after 10 days
- confirm that the incident is not resolved, the ticket will be moved back to an *in progress* state
- any ticket for an incident or service request in a *waiting* state with a *waiting on customer* reason which has no updates for 5 days will automatically move to a *resolved* state, then move to *closed* state automatically after 10 days.
- make updates which restarts the 5 day clock, for example additional comments being added to the ticket
- a change in state on the ticket will cancel this functionality.

6.6.4.4 Incident Reporting

You are notified of all incidents via a notification email, which, for security purposes, contains minimal information, with the full incident details only available via Manage Centre.

6.6.5 Capacity Management

Note. NTT is not responsible for capacity management of third party SaaS applications.

6.6.5.1 Capacity Monitoring and Reporting

The monitoring systems utilized within the service regularly check a number of telemetry points. Through continuous monitoring, NTT is 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, a disk filling with log data. Using this as a starting point for incident management, NTT will work with you to advise on potential resolution or mitigate the risk.

6.6.6 Capacity Improvement Recommendation

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

- request you to change the logging levels or to network architecture
- request you to change the monitoring levels within the configuration item (for example turning off debug logging)
- request you to update hardware or licenses to facilitate greater capacity.

6.6.6.1 Capacity Planning

With the trend data available, NTT, partners, and/or clients may make decisions about future requirements and expected growth. This provides invaluable forward planning to those responsible for budgeting or capacity planning. For example, Trend Analysis Reports will show disk consumption over time, which could be an indicator of a need to procure new hardware or additional storage in the next budgeting cycle.

6.6.6.2 Capacity Change Implementation

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

6.6.7 Asset Management

You are responsible for hardware upgrades of the underlying infrastructure that houses your SIEM. NTT is responsible for “OS Up” patch management that includes the SIEM application and modules installed.

Note. Asset management is not applicable for SaaS applications.

6.6.7.1 Configuration Item Recording

NTT records and tracks your in-scope configuration items with information available within Manage Centre.

6.6.7.2 Configuration Item Control and Updates

Minor Version, Patch and Security Hotfix

NTT monitors Original Equipment Manufacturer (OEM) published patch, security hotfix, and version updates associated with the in-scope configuration items. NTT also reviews such releases for applicability. If NTT determines that such updates or patches are recommended for security or operational reasons, NTT shall request approval prior to implementing any such update(s) through an NTT-sourced change ticket. For more information, see *NTT-Sourced Requests*.

NTT will install a software patches and application minor version upgrades for your SIEM. All patches or minor version upgrades are considered normal changes and will follow the change management process.

If NTT determines that an in scope configuration item is susceptible to a new vulnerability, which is classified as low or medium, NTT will seek your approval prior to taking any response steps. In the event that a SOC engineer

deems a new vulnerability as high in severity, NTT may take immediate response steps through an emergency RFC.

Major Version Upgrade

Major version upgrades to your devices under management require careful planning, coordination, management, and roll back planning. NTT considers all major version upgrades to SIEM configuration items under management as high risk as they pertain to yours production environments. Therefore, major version upgrades are considered Project Oriented Requests (PORs),

NTT will coordinate all major version upgrades with you and may agree to utilise the SOC and MACD service units, propose a fixed price project, or perform the work on a time and materials basis.

Content Update

Each SIEM vendor provides clients with periodic updates about upgrades and patches to the SIEM platform.

Updates

Where applicable, updates in terms of detection capabilities provided by the SIEM-vendor are usually automated and require connectivity between the configuration item and the Internet to download the updates. NTT checks that automated updates provided by the SIEM vendor are being downloaded and installed successfully.

Failures

If the content update fails, an incident is raised on your behalf. Subsequently, any errors related to a configuration item's ability to update the signatures is resolved using the standard incident management process.

Client Responsibilities

You must ensure that all the configuration items are connected to the Internet in order to enable the delivery of automated content updates from the configuration item manufacturer.

Implied Service Level Agreement

If the failure of a signature update mechanism is diagnosed as a manufacturer-related incident, the service level to resolve the incident will be in accordance with that manufacturer's third party supplier agreement.

6.6.7.3 Configuration Item Backup

NTT will perform daily backup of the SIEM configuration items. The backup files are stored on client-owned storage. NTT will also perform backups of the NTT proprietary technology (CTS and Security Appliance).

6.6.7.4 Configuration Item Restore and OOB

The Remote Management Kit (RMK) provides Out-of-Band (OOB) management of configuration items. It is not applicable or supported for virtual or cloud-based configuration items.

The RMK is optional and not required for SOCaaS.

OOB management is utilized to perform remote troubleshooting and maintenance activities if any of your configuration items encounter a catastrophic failure or lose connectivity to your network.

The RMK is under complete control by us. You must not:

- direct any unauthorized traffic to the RMK
- attempt to login to the RMK
- tamper with the RMK
- attempt to perform any penetration test on the RMK without express written consent from us.

Should both the primary and OOB solutions become inoperable or otherwise unavailable for our use, NTT reserves the right to suspend the Service for the applicable configuration items until the situation is remedied. We are not responsible for any incident involving a configuration item while connectivity to the RMK is unavailable.

The RMKs are monitored and managed as part of the service.

6.6.8 Configuration Item Status Reporting

Configuration item status reporting is available via Manage Centre. Status reports include version details and traffic light status.

6.6.9 Configuration Management

6.6.9.1 Service Request Fulfilment

Service request fulfilment focuses on requests related to configuration of the SIEM, for information, advice and access. There are also other service request types available related to more generic questions.

Service Request Management

Service requests are raised via a ticket in Manage Centre.

Service Requests regarding changes to the SIEM configuration, including fine-tuning of rules, creation of custom use-cases, dashboards, reports and log parsers are administered through the MACD service unit model as described in *6.6.9.2 Move, Add, Change, Delete (MACD) Fulfilment*. A full list of available MACD service Requests are found in *Appendix A*.

NTT tracks, monitors, and reports the attainment of various key performance metrics on a monthly basis.

Request for Information

You may request information about the performance, configuration, or other aspects of in-scope configuration items through Manage Centre. NTT shall provide the information in the service request.

Service Request Reporting

All incidents and service requests are recorded and reported back to the Client through the Manage Centre Portal.

Project Oriented Request (POR)

NTT will charge, and you agree to pay, the then-current applicable hourly rates for work associated with PORs. If any change performed by you results in adverse effects and requires remediation work to be performed by NTT to restore the software/configuration item to proper working service, you agree to pay NTT the then-current engineering hourly rate to return the affected device to normal operating run-state.

6.6.9.2 Move, Add, Change, Delete (MACD) Fulfilment

Change and Service requests are administered through a MACD service unit model and are requested via Manage Centre.

MACD service units can be used across different MSS-services provided by NTT. MACDs are deducted in the execution of any client-sourced service requests pertaining to a RFC of configuration items. The number of MACD service units deducted per service request is based on a predefined list of standard tasks that NTT has derived assessing the level of complexity to route accordingly to an appropriate SOC engineer.

Where the usage of MACD service units for a service request exceeds 6 hours of effort, NTT may charge additional MACD service units or propose a POR to perform the work on a time and materials basis.

NTT tracks the MACD service unit usage and includes it within any scheduled service reviews to ensure that your account is operating in line with MACD availability. If the MACD service unit balance drops below a certain threshold, you will be notified for purchase of additional MACD service units.

See *Appendix A* for more information.

Non-standard Tasks Utilizing MACD Service Units

If there is no pre-existing menu item for your request, NTT considers this a non-standard task.

NTT will review the non-standard tasks requested by you to determine:

- the apparent risk associated with performing the task
- the likely impact of the change
- if NTT have the appropriate skills to action or implement the task
- If the non-standard task should become a standard task (based on demand/repeatability)

NTT will assess the non-standard task to determine the correct number of MACDs. NTT will then provide you with the number of MACD service units that the task will incur for approval to proceed. Once approved by you, NTT will execute the request for a non-standard pre-approved task. No service levels will apply to the execution of a non-standard task.

6.6.9.3 Change Management

At your request, NTT will implement a change to in-scope configuration items in accordance with an associated MACD task or non-standard task requests. Creation of, and updates to dashboards, reports, rules, use cases, etc. are requested via Service Requests as outlined in Appendix A.

Client-sourced Requests

A valid client contact must submit a RFC within Manage Centre.

NTT-Sourced Requests

NTT may submit a RFC when a change is necessary to resolve a problem or incident.

Change Reporting

Manage Centre is used to report and track all changes.

The party making a change is required to open an applicable RFC in Manage Centre prior to implementation to ensure coordination between both parties.

Request for Change (RFC)

All RFCs follow the change management process as outlined below and require approval by NTT.

There are three types of RFC. These are:

Normal Change

Normal changes require approval, from both NTT and you, respectively, before the defined change is implemented. NTT is not authorized to apply changes on your behalf without documented consent from your authorized individuals (documented within a Change Approver Group on Manage Centre) from both parties via a RFC resident in Manage Centre.

Standard Change

When a standard change ticket is raised via Manage Centre, NTT is authorized by you to apply changes without authorization. However, the NTT internal approval process is still valid.

Emergency Changes

An emergency change is considered a RFC that must be implemented as soon as possible, for example, to resolve an incident or to implement a security patch. NTT will work with you during the change management process.

Cancelling a RFC

You may cancel a RFC up to 4 hours before any scheduled change is committed to the device's configuration. In this case, any MACD credit that would have been deducted shall be cancelled.

If you would like to reverse a change that has already been implemented, you must submit a new RFC via Manage Centre. In this case, the commensurate MACD credits shall be deducted for both the original change and any subsequent reversal requested.

Change Implementation

Depending on the risk associated with the change, NTT will perform one or more of the following tasks associated with each change:

- Backup the current running configuration(s) prior to change
- For SaaS applications where the vendor does not support backup and rollback, ensure that all changes are documented so that the previous change can be identified and reverted
- Ensure a copy of any applicable software is readily accessible
- Ensure a rollback plan is documented if there are issues with the change
- Assign an internal ticket number (if applicable) to track the change for auditing purposes
- Implement and test the change (as far as is possible – testing responsibility is also shared with you) to confirm whether the change met the requirements as specified by the submitter
- Create a backup of the new configuration after implementing the change
- Update NTT's service request ticket indicating whether the change was successful or not

Exceptions

You understand that any exceptions that may arise due to deviation from or circumventing the processes described herein may result in an unstable and/or unsecured configuration item(s) and/or non-compliant configuration(s). Accordingly, you release NTT from any liability resulting in outages, misconfigurations, exposures, loss of business, or other negative impacts directly related to any action made by you.

You agree that any work performed by NTT to troubleshoot issues that are directly attributable to your action is billable at NTT's current engineering hourly rate.

Change Impact Analysis

As part of the change design process, NTT conducts a Change Impact Analysis in accordance with all the RFCs (pre- and/or post-implementation). The analysis is conducted prior to the implementation of any RFC, including patch and version management, or PORs to ensure:

- Hardware/software meets all prerequisites
- Backups of previous version/configuration exist (if applicable)
- Any change is consistent with the security best practices and does not compromise the client's network, service, or that of NTT
- Any change is relevant to the client's environment
- Any change can be implemented within the requested timeframe

NTT reviews incident tickets, service requests, and documentation regarding the RFCs and may seek clarification.

7 Service Decommission

Should your data be resident within your own estate or environment, you shall retain all data. NTT brings in metadata that can and will be purged upon completion of the contract. NTT will work with you to remove all accounts on your SIEM to prevent NTT from being able to access your SIEM. NTT will also provide instructions to decommission the Security Appliance and CTS. There are multiple scenarios, each with their own nuances. These scenarios are described below.

- Scenario 1 – Client SIEM exists within its own estate ○ NTT will decommission the Security Appliance and CTS
  - NTT will purge all metadata from backend systems
  - Client will retain all log data within the SIEM
- Scenario 2 – Client SIEM is hosted by NTT ○ NTT will decommission the Security Appliance and CTS
  - NTT will purge all metadata from backend systems
- Scenario 3 – Client is on third party SaaS ○ NTT will decommission the Security Appliance and CTS
  - NTT will purge all metadata from backend systems
  - Client will be responsible to transition all logs, data, and rules to new capability

8 Service Prerequisites

8.1 General Requirements

8.1.1 Delivery Model

The standard delivery model shall be 24 hours a day, 7 days a week leveraging NTT's Global SOCs. Deviation from this standard shall only be considered on a case-by-case basis and must be supported by a completed application for non-standard services. NTT shall consider the request and its associated cost implications and, wherever possible, strive to meet the requested requirements. However, NTT reserves the right to refuse any request for a deviation from the standard delivery model.

8.1.2 Software and Appliance License

You are responsible for valid manufacturer product license(s) that are required for all components (including security application and operating system) of the SIEM environment under management for the duration of the service contract period. You must ensure that licenses are valid at the start of the service contract through to the end of the service contract and that the correct licenses are purchased and installed

8.1.3 Manufacturer Hardware and Software Support

Managed configuration items must have full manufacturer support at all times during the service contract period. The manufacturer support contract must have Partner Enablement, where applicable. In order to raise support tickets with the manufacturer on your behalf, NTT must be added as an authorised vendor support contact and/or partner. You must include NTT as an "authorized agent" for the support contract so that NTT can raise vendor tickets.

NTT shall not provide any services for any configuration item not covered by a valid maintenance contract. Neither shall NTT manage any configuration item where the software or hardware has been declared *end of life* or *end of support* by the manufacturer, prior to the start of any contract or subsequent 12-month renewal period. The service does not include the replacement of obsolete hardware/software.

8.1.4 Software Modification

NTT shall not support altered, damage or modified software or software that is not an NTT-supported version. The SIEM environment will be on the current vendor supported version, or one version behind. (N / N-1).

8.1.5 Software Updates (Subscriptions)

You are responsible for all manufacturer's software subscriptions (for example, software updates) for any configuration items to be managed. Such subscriptions are required for the duration of the service contract period. You must ensure that any software subscriptions are valid at the start of the service contract through to the end of the service contract. NTT does not provide any services for expired subscriptions.

8.1.6 Limitations of Use

Only the manufacturers' security application/OS software, relevant and/or necessary software/applications and software provided by NTT (where applicable) to support NTT's service may be run on the configuration item.

8.1.7 Privileged Account Management (PAM)

NTT will utilize a PAM solution in order to efficiently scale from client to client for authentication into a client environment.

8.1.8 NTT Security Appliance Virtual Environment

All environments provided by you for NTT's Security Appliance must adhere to specifications outlined within the latest 'NTT Appliance Installation and Configuration Guide', which can be found on Manage Centre. In addition, proactive monitoring of any shared resources (for example, CPU, memory, network, and storage) is your responsibility to ensure a stable virtual environment. Any hardware or software issues relating directly to the environment are your responsibility; however, NTT will work with you to resume normal operations in the event of appliance-related failures.

8.1.9 Designated Security Contacts

You must provide a minimum of two staff members to be the security contacts and, if applicable, a service desk contact that NTT will liaise with to deliver the service. You must provide full contact and authentication details for each of the security contacts and this must be included within the Transition Workbook.

8.1.10 Administrative Privileges

NTT requires full and exclusive administrative, root privileges for all in-scope configuration items for the service contract period.

8.1.11 Client Staff and Resources Requirements

You shall provide knowledgeable technical staff and/or third party resources to assist with hardware and software implementations, including:

- Configuring end-to-end connectivity to ensure the successful transport of all in-scope log feeds and evidence data
- Providing rack space and power for each in-scope NTT Security Appliance , if applicable
- Providing an IP address for each Security Appliance to be installed at your site
- Installing the Security Appliance on your network
- Placing the virtual CTS image in your virtual environment in accordance with NTT's instructions
- Participating in calls with third party vendors and offering support, as appropriate

Cloud Specifics

- Configuring identity access management roles and account as directed by NTT
- Ensuring NTT SOAR API can access the cloud service provider tenant account(s)

8.1.12 Technologies that may Impede Delivery

If you utilise security technologies that block traffic, rotate logs, or otherwise impede NTT's ability to receive logs from the in-scope devices, you must notify and cooperate with NTT to identify and develop a mutually agreed-upon mitigation.

Note. Loss of log lines and interruption of monitoring capabilities may occur because of uncoordinated log rotation.

8.1.13 Third Party Vendor

You shall work directly with your third party vendors that host any in-scope devices to allow NTT to deliver services.

8.1.14 Third Party Device Failure

You shall work with your third party vendors to rectify the failure of all the devices that have not been provided by NTT and are responsible for all associated expenses.

8.1.15 Internet Service Provider or Client Network Outages

You are responsible for resolving your Internet Service Provider (ISP) outages, or issues with your internal network infrastructure.

8.1.16 System Backups

NTT recommends that you perform full backups of the relevant systems prior to the onboarding of services.

8.1.17 Closure of Incident and Security Incidents

You shall work with NTT to bring closure to each incident and security incident identified by the services presented in this Service Description.

8.1.18 Providing Required Information

Failure by you to provide any of the service requirement information on a timely basis can result in delays in service transition and service delivery by NTT and NTT shall not be liable for any consequences of such delays.

9 Service Management

As a Client of SOCaaS, you will be assigned an Information Security Engineer and 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 Management Service (TAM) function as described in 9.3 below.

9.1 Information security engineer (ISE)

The NTT Information Security Engineer provides technical expertise in relation to the your SIEM solution. An ISE is assigned during Service Transition and will act as a trusted advisor and technical liaison between you, as well as the Service Delivery Manager. Please refer to Service Appendix C for an overview of the meeting schedule and participants list.

9.2 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 NTT SDM include:

- Establish client relationship
- Capture and manage minutes, agenda items, actions, and decisions
- Change management issue management
- Escalation management
- Risk management
- Service level monitoring, reporting and management
- Service review meeting

9.3 MSS Technical Account Management Service (Option)

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 Management Service team leverages security best practices and an expansive knowledge base to deliver globally consistent security programs tailored to specific client 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 Management Service team are an additional component of the NTT MSS delivery model who provide cybersecurity insights beyond the MSS services. Coupled with NTT's 24/7 SOC teams, the MSS Technical Account Management Service provides operational support and consultative guidance in alignment with your business priorities and technology roadmaps.

The MSS Technical Account Management Service 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 benefit from the MSS Technical Account Management Service team support of internal and external stakeholder management while you face challenges implementing security controls across your enterprises.

The MSS Technical Account Managers are the client advocates who identify and track action items and service requests that have been raised via the NTT Service Desk to reduce the time to respond to client requests. The MSS Technical Account Manager Service team also provide a quality control function to ensure delivery excellence, maintain high levels of client satisfaction, achieve project successes, and drive continual service improvement.

The SOC provides 24/7 support for clients and although the MSS Technical Account Management Service team are not a 24/7 resource, the MSS Technical Account Management Service 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.

10 Changes in Service

10.1 Regulatory Change Requirements

If regulatory changes (for example, changes by a regulatory agency, legislative body, or court of competent jurisdiction) require NTT to modify the services described herein, NTT will modify the services and this Service Description accordingly without diminishing the features, functionality, or performance of the service. In the event of a modification in response to regulatory changes results in a diminishment of features, functionality, or performance, you agree in good faith to work with NTT to amend this Service Description accordingly and

execute any additional agreement, which may be reasonably requested by NTT to document such an amendment.

10.2 Method of Service Delivery

NTT reserves the right to make changes to the service, provided these changes do not have a material adverse impact on the functionality or performance.

11 Service Exclusions

Unless otherwise agreed between the client and NTT, the services described in this document do not include:

- Configuration of log sources that feed the SIEM environment
- Support and Remedial Work, which is not expressly stated in this Service Description. This includes any troubleshooting and problem solving related to issues arising from the Client's actions or Client's network
- Project Oriented Requests (PORs) are not included in the Services described herein and are subject to additional fees. NTT and the Client will develop a scope for the PR and NTT will provide a separate quote to the Client, which must be executed prior to performance of any such work
- Client requests for advice or consultation regarding network or configuration item configuration not specifically outlined in this Service Description are subject to additional fees
- Client staff training unrelated to NTT services (NTT provides written and video training on Manage Centre Portal and the different functions that the Client may use within the portal)
- Software or hardware maintenance (unless otherwise stated)
- Software licensing (unless otherwise stated)
- On-site forensic services
- Security policy or procedure establishment
- Remediation of a security incident or attack on your network, server, or application unless purchased as part of an optional package

Appendix A MACD Table

Service	MACDs
Client Training	54
Rule Creation	10
SIEM Hierarchy Add/Change	5
List Changes	10
XSOAR/SIEM Custom Scripting	54
Custom Parser Creation	Custom[2]
User or Role Add/Remove	7
Tuning	10
Log Source or Agent Add/Remove	5
Dashboard (Web UI) Creation/Change	13
SIEM Report Creation/Update	8

[2] Depending on the complexity of the task, the number of MACDs deducted will vary from case to case. Very complex parsers may be delivered as a Project Oriented Request instead of using MACDs

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 – Response	NTT will assign an Incident ticket with priority ____ within ____ minutes of receiving the ticket at NTT`s Service Desk.	P1&P2	30 Min	N/A	N/A	
		P3&P4	60 Min			
Incident Management – Resolve	NTT will resolve a priority ____ incident within ____ hours of receiving the ticket at NTTS Device Management Team.	P1	8 Hours	N/A	N/A	
		P2	16 Hours			
		P3&P4	48 Hours			
Emergency Change Response	NTT will assign an Emergency Change ticket within ____ minutes of receiving the ticket at NTT's Service Desk	N/A	30 Min	N/A	N/A	N/A
Change Response	NTT will assign an Change ticket within ____ minutes of receiving the ticket at NTT's Service Desk	N/A	60 Min	N/A	N/A	N/A

Category	Description	Priority	SLA	Service Credits	Service Credit Limit	Service Calendar
Change Implementation – Complete	NTT will complete changes before the end of the change window as mutually agreed upon between client and NTT.	N/A	95%	N/A	N/A	
Resolve Notification (Service Level Objective) – Notify	NTT will provide a resolve notification for every Incident ticket within ____ minutes of restoring the service.	N/A	30 Min	N/A	N/A	

Table 4 Service Level Agreements

Appendix C Service Governance

Timeframe	Attendees	Summary
Weekly	SDM ISE Client POC TAM (optional)	Discuss day to day operational issues and/or challenges. Review current rule sets, reporting, and use cases as well as tuning or potential tuning opportunities. Review new threats, or potential threats which may affect the client.
Monthly	SDM ISE Client POC Client Sponsor TAM (optional)	Overview of previous month's metrics, as well as discussion in relation to current and upcoming projects.
Quarterly	SDM ISE Client POC Client Sponsor Client Executive NTT Executive NTT Sales Representative TAM (optional)	Quarterly business review to go over previous quarter's metrics, review completed and upcoming projects, as well as roadmap items for the upcoming quarter.

Table 5 Service Governance