Standard Integrated Security

The complete service is defined by the combination of the following items for which the specific selection must be in In Scope in the SOW:
Client Service Description –service delivery operations that are common to all NTT Managed Services
Service-Specific Operations – service delivery operations that are specific to *Standard Integrated Security*. These operations are additive to the *CSD Client Service Description.*

1 Overview of the Service

With the Standard Integrated Security service NTT embeds security functions into the range of managed solutions hosted on our supported managed services platforms.

NTT employs a “secure by design” philosophy where we include security services for fully managed solutions hosted on our supported managed services platforms. Standard Integrated Security services provide Security Logging and Retention, Security Information Event Management (SIEM) and Reporting, Security Operations Center (SOC) detection and notification services, and Endpoint protection.

The following environments are supported:

(a) NTT Managed Services Platform (MSP)

(b) NTT Managed Private Cloud (NTT Anywhere)

(c) NTT Managed Public Cloud (limited locations and must be specified in the SOW as in scope)

The following service elements are included in the Standard Integrated Security service. Additional services may be purchased separately.

1.2 System Logging and Retention

NTT performs 24x7 security monitoring and logging for managed systems specified as in scope in the SOW. Logs are maintained in archive for forensic and root cause analysis. Application, Security, and System logs that are in scope are captured in a central repository and are maintained for only one year if logging events require investigation. NTT assumes a log threshold per OS, device type, and in-scope services in NTT sole discretion. Please see Statement of Work for details of Log Type to be collected in Scope, otherwise all items are out of Scope.

NTT will collect the following log types:

Log type	Description
OS-Level Logging	Collect and off-load NTT supported server operating system (OS) logs to log data repository using NTT default logging policies. Windows logging includes Application, Security, and System events. Linux logging includes Syslog, Secure Log, and Audit log from the /var/log/ directory.
Security Product Logging	Collect logging from security-oriented products. This includes perimeter defense products (such as firewalls) to security application products; both base level products (such as AV) and subscribed products (such as web gateway or FIM). Log sources supported are those native by logging system only. The specific product must be specified as in scope in the SOW otherwise it is out of scope.

NTT will monitor logs for the following activity:

(a) User activities

(b) Logon attempts (successful or unsuccessful)

(c) Changes to, or attempts to change, security settings and controls

(d) Exceptions

(e) Information security event messages

(f) Operational events

Upon client request, NTT will transmit a copy of logs for in scope Security Services to the Client in an industry standard format.

1.3 Additional Services (Security Logging and Retention)

NTT can collect database audit logs (login/logout/user activity) from Oracle and MS SQL Databases and review audit activity (This requires additional database logging configuration and storage sizing). This additional service incurs additional service fees and it is out of scope unless identified as in Scope in the SOW.

1.4 Security Information Event Management (SIEM) Service and Reporting

NTT will perform SIEM services to collect security log events from numerous sources across an enterprise and store the data in a central location in NTT's discretion.

NTT will perform the following tasks in this Service:

Task	Description
SIEM Log Correlation and Alerting	Import security log information into NTT managed multi-tenant SIEM for correlation and alerting up to the assumed log baseline threshold.
SIEM Alert Tuning	Maintain alert tuning, false positive tuning, and event tuning, on a regular basis for NTT managed SIEM.
SIEM Threat Feed	Maintain and apply NTT provided 3rd party threat intelligence feeds into SIEM for correlation. NTT provided threat feeds are provided in NTT's sole and absolute discretion.
SIEM Security Alert Investigation	Initial investigation into security events of NTT managed systems based upon triggered SIEM rule(s). The investigation is to discern the validity of the alert and initial details of the event for Client notification. If the initial investigation is declared an incident, then NTT will initiate and follow its Security Incident Response process.
SIEM Reporting	Base level SIEM reporting provides visibility into logs collected, alerts generated, environment baselines, and data trends.

1.5 Additional Services (SIEM service and reporting)

NTT is able to offer the following additional services. These additional services incur additional service fees and it is out of scope unless identified as in Scope in the SOW.

(a) SIEM Custom Log Import - Creation of custom SIEM log parsing rule to ingest data into the SIEM for security evaluation.

(b) Client supplied threat feed is out of scope and not available to be used unless Client purchases dedicated console.

(c) Security Logging Visibility - Provide one (1) Executive Cyber Health Summary report per month for the services/systems subscribed and under management by NTT.

1.6 Security Operation Center - Detect and Notify

Upon alert or notification of a potential security incident of NTT managed systems, the NTT SOC will conduct an initial investigation into alerts or notices it receives from NTT-managed alerting systems or directly from the Client for validity and an initial impact assessment.

NTT will perform the following Tasks:

Task	Description
Initial Security Incident Triage	Upon alert or notification of a potential security incident related to NTT-managed systems, NTT will do an initial investigation into alerts or notices. The data collected is provided to the Client at the initial notice of the incident, which takes place within the time frame specified in the MSA. Determinations on alerts / notifications that were not incidents can be represented via reporting. NTT shall perform all Triage in its sole discretion.
Security Incident Response Process	NTT will support the Client's security incident response process per the NTT Client Security Incident Response Process as applicable to the scope of the Services provided.

1.7 Endpoint Protection

NTT installs Antivirus software on all systems that are in Scope in the SOW for this Service. Additionally, NTT installs Endpoint Detection and Response software, on managed servers that are specified as in scope in the SOW. This provides continuous, endpoint visibility that spans detection, response and forensics. Additional use may result in additional Fees for usage.

NTT will perform the following Tasks:

Task	Description
Provide Server Security Protection Suite License	Provision of a License from a 3rd party standard Server Security Protection Suite used by NTT (the "NTT Server Security Protection Suite") for in-scope NTT managed servers.
Deploy and Manage Server Security Protection Suite	Deploy and manage the standard NTT Server Security Protection Suite to in-scope NTT-managed servers.

Monitor and Update Security Definitions	Monitor and update remote security definitions daily or as new emergency security definitions become available for in-scope NTT-managed servers.
Alerting Integration	Integrate alerting for the supported NTT Server Protection Suite into the NTT ITSM (ticketing system) or SIEM (up to the assumed log baseline) for centralized response.
Server Protection Platform Update	Where required and when necessary, update the Server Protection Platform to the latest vendor-recommended release.
Global Exclusions Policy Configuration	Initial configuration of Global Exclusions Policy and Client-specific Exclusion Policy.
Global Exclusions Policy Maintenance	Maintain a Global Exclusions Policy, as well as Client-specific Exclusion Policy.
Global Exclusions Policy Management	Manage the Global Exclusions Policy or Client-specific Exclusion Policy, up to the hours purchased per the Fees Schedule in the SOW.

1.8 Additional Services (Endpoint protection)

NTT is able to offer Endpoint Protection for regulatory environments (Gov Cloud). These additional services incur additional service fees, and it is out of scope unless identified as in Scope in the SO

2 Client Responsibilities

The Client is responsible for the following functions throughout the entire service lifecycle:

Service element	Client Responsibility
Security logging and retention	Security Log Import - Ensure that the client can accept NTT-transmitted logs in the industry standard format provided
	Security Log Import - Ensure that the client has the proper network connectivity in which to accept the logs
	Custom Application Log Parser - Document logging output format and log structure of the custom developed applications or platforms as it pertains to the SIEM
	Custom Application Log Parser - Provide the data layout of the log structure and any updates as they are generated.
SIEM	Provide the log structure standard if the application is custom developed
Detect and notify	Leads the security incident response process upon receiving notification
	Coordinates the quarantine and restoration steps with the NTT Client Delivery Manager and NTT and Client IT operations teams for in scope services
	Request additional access to Client systems for quarantine, installation of investigative software, or for manual investigation purposes.
	Determine the scope and business impact and if required declare a Security Incident or a false alarm at the time of Initial notice from NTT
Endpoint protections	Provide timely change windows and appropriate testing of new versions within its environment.

	Specify exclusions for non-NTT-managed applications and provide appropriate testing of exclusions within the environment
	Comply with any applicable third-party license terms and conditions related to the NTT Server Security Protection Suite.

3 Limitations

The following limitations are in place throughout the entire service lifecycle and out of scope:

Service element	Limitation
Security Logging and Retention	Additional Log Retention is out of scope but available to Client for additional storage fee
	Additional Non-OS security logging is out of scope but available for additional fee
	Client-Managed Security Product Log Retention is out of scope but available to Clients for additional fee
SIEM	SIEM Data Access - Console Access by Client or Client 3rd party is not supported
	Custom SIEM Reports - Creating custom reports if standard Security Logging Visibility reports do not contain the information required is out of scope
	Additional Log Retention is out of scope but available to Client for additional storage fee