Enhanced Security Services - Dedicated Security Information Event Management Service and Reporting

1 Overview of the Service

NTT will perform Security Information Event Management (SIEM) services to collect security log events from numerous sources across an enterprise and store the data in a central location. Consolidating the data allows for centralized reporting and analysis, providing an enhanced level of threat and incident detection.

(a) NTT's SIEM solution provides the Security Operations Center (SOC) with an integrated view of the entire cloud environment.

(b) 24x7 NTT SOC monitoring and responding to security events.

(c) NTT can integrate Log Sources and has many out of the box industry leading vendor technology integrations.

2 Customer Responsibilities

Client to provide the log structure standard if the application is custom developed.

3 Service Specific Operations

Service	Description
SIEM Log Correlation and Alerting	Import of security log information into NTT managed Client dedicated SIEM for correlation and alerting up to the purchased events per second (EPS) threshold. True-ups may be required if the purchased EPS is exceeded.
Client Access	Upon request, NTT will grant access to Client for custom reporting, and in good faith Client will not develop any queries that would cause harm. If a Client written report causes disruption to Service, the SLA for the specific service would not apply.
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.
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.

4 Services Available for an Additional Fee

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

(b) SIEM Threat Feed - Client supplied threat feed is available with purchase of 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.

5 Supported Environments

(a) NTT managed client on-premises data center

(b) NTT managed private and public cloud

6 Out of Scope

Enhanced Security is not a standalone offer, and can only be included when standard security is in Scope in the SOW