Enhanced Security Services - File Integrity Monitoring

1 Overview of the Service

NTT manages a File Integrity Monitoring (FIM) solution which examines operating system, database and application software files to see if and when they change, how they change, who changed them, and provide potential options if any, to restore those files if those modifications are unauthorized. Deployment of FIM technology provides the protection of IT infrastructure, change intelligence along with business context and remediation steps and help to meet regulatory compliance standards like PCI-DSS, FISMA, SOX, NIST and HIPAA. This service must be specifically selected as in scope in the SOW.

2 Client Responsibilities

(a) File Integrity Policy - Client to Identify files, file directories, and devices to be monitored.

(b) Monitor and Reconcile Changes - Client to review File Changes and provide information to NTT Security Team on actions that are unauthorized and require investigation.

3 Service Specific Operations

Task	Description
File Integrity Monitoring	Monitor up to fifty (50) files per managed server as frequently as a one (1) hour interval.
Alert	FIM Alerts will be configured to be sent via email to Client-specified group upon changes.
Alert	FIM Alerts can be configured to be sent to ITSM (ticketing system) for an automated ticket creation.
Log Retention	Logs will be kept for one (1) year unless another time period is agreed upon under this SOW for Long Term Retention.

4 Services Available for an Additional Fee

(a) Database Monitoring - Monitor and report on Database settings/configuration changes.

(b) Active Directory Monitoring - Monitor and report on Active Directory changes.

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.