

## **Log Management Services**

Over the past several years, heightened requirements to provide evidence of vigilance in computer security practices have increased the need for better computer system log management practices.

In addition to the fiduciary responsibility, government must comply with a multitude of compliance requirements (e.g. TAC 202, SOX, HIPAA, PCI, FISMA and GLBA).

Increased vigilance has resulted in more log aggregation, longer and more secure storage and protection, higher frequency reviews, normalized format and increased volume requirements. Industry best practices recommend centralized aggregation, archival, and analysis as basic functionality of any IT infrastructure.

There are three main sub components of CGI security services Log Management Service offering:

- Log Aggregation and Consolidation
- Log Archiving and Protection
- Log Monitoring and Reporting

CGI's scalable Log Management Service provides a way to collect and centrally aggregate logs, to quickly browse through large amounts of data required during investigation, to produce reports, to analyze and correlate the logs in order to identify malicious activities and attack patterns and to alert on specific criteria customized to each Client's environment.

## **Benefits**

- Centralized log collection
- Log Archiving and Compliance
- Litigation quality log retention
- Real time correlation and analysis of events
- Pre set of Policies and Reporting Configurations
- Monitoring the Log Management components themselves for operational and security issues
- Continuous verification that the Log Management is functioning properly (rule configurations, integrations)
- Vendor Management activities (updates, testing, notifications)