LTS Secure
SECURITY ANALYTICS

Security Analytics

Collect and Process:

Security Analytics helps parse and enrich logs, wire data, and event data from any data source. LTS Secure Security Analytics also provides centralized configuration management for 3rd party collectors such as beats, fluentd and nxlog. The processing pipelines allow for greater flexibility in routing, blacklisting, modifying and enriching messages in real-time as they enter into LTS Secure solution.

Analyze and Search

LTS Secure Security Analytics searches through terabytes of log data to discover and analyze important information. It uses the powerful search syntax to find exactly what you are looking for. It also saves search queries to share.

Drill-Down and Visualize

LTS Secure Security Analytics creates dashboards to visualize metrics and observes the trends in one central location. It uses field statistics, quick values, and charts from the search results page to dive in for deeper analysis of your data. The simple user interface enables team members to easily access the wealth of information and add new charts.

Alert and Trigger

LTS Secure Security Analytics triggers actions or get notified when something needs attention, such as failed login attempts, exceptions or performance degradation.

Users and Roles

It allows group users into roles to simplify permission management. You can also restrict what kind of log messages certain users are allowed to access, using our real-time categorization functionality.

User Context

LTS Secure Security Analytics can be integrated with your existing LDAP user directories to do behavior and user context analytics.

HIGHLIGHTS

- Collect and Process

- Analyze and Search

- Drill-Down and Visualize

- Alert and Trigger

- Users and Roles

- User Context