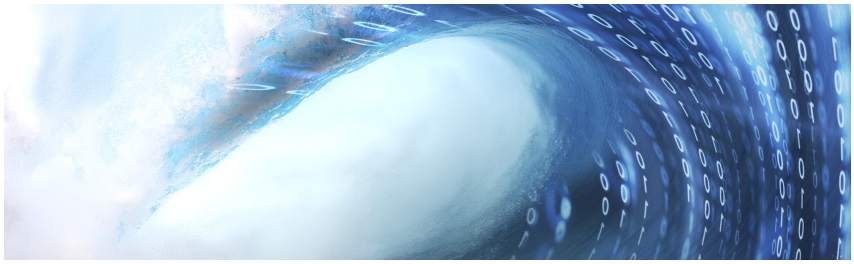
Salient CRGT Splunk Services



Taming a Tsunami of Data Using Splunk Analytics

Organizations are experiencing exponential growth of automated data capture and retention, generated both within and outside corporate boundaries. The correct methodology and tools can navigate this ocean of bits and bytes. Salient CRGT, in partnership with Splunk, provides end-to-end business analytics. Based on Splunk Enterprise, our analytics capability addresses multiple use cases that span organizational data silos, collecting and analyzing large-scale, product agnostic, structured and unstructured data.

Salient CRGT pioneered the use of Splunk for a large logistics organization, analyzing log files from mission-critical systems to generate ongoing operational metrics, including web and security analytics. Apps built using Splunk continually monitor business systems for performance degradation, and provide proactive alerting. These apps are also able to integrate with the customer's ticketing system for automated problem ticket generation and assignment. Consequently, the customer has seen marked improvements to both operational visibility and performance for its applications.

Below are a sample of Salient CRGT's Splunk apps and capabilities developed for one of our larger customers.

Salient CRGT's Splunk services have:

- Installed and implemented a unified SIEM (Security Information and Event Management) solution for a large federal agency capable of receiving 10 terabytes of data per day from over 600 disparate systems and 50 data sources.
- Provided "single pane of glass" visibility to multiple operations teams for critical incident analysis, troubleshooting, and remediation at a large retail organization, reducing both cost and time to incident resolution.
- Created an innovative Splunk overlay of sales transaction data to detect fraud by statistical and predictive analytics.

Splunk Enterprise Security

Challenge – Security Information and Event Management (SIEM) solutions provide security monitoring for cyber-attacks and data leaks, and to maintain controls compliance. However, such solutions can be complex, take too long to deploy, produce unwieldy amounts of data, and require enormous manual effort to tune out noise, e.g., false positives. Many current SIEM products also fail to sufficiently address cloud applications. Further analysis often requires a third-party big data provider to distill valuable and actionable information from large amounts of captured data.

Salient CRGT's Approach – Salient CRGT assisted in mitigating its customer's SIEM challenges by architecting and deploying a clustered Splunk Enterprise environment of approximately 100 servers capable of indexing up to 10 terabytes of data per day. Splunk ingests over 50 different data source types from over 600 distinct hosts including network components, intrusion detection/prevention systems, anti-malware solutions, web and email proxies, mobile device management, and application servers.

The agency's Corporate Information Security Office (CISO) leverages Splunk Enterprise Security (ES), providing a complete Big Data SIEM solution for investigating security incidents such as suspicious access attempts, malware events, and malicious email traffic. As a Splunk implementation partner, Salient CRGT incorporated new data sources by determining data transmission methods, wrote technical add-ons to correctly parse events, provided alerts and dashboards to the data owners, and ensured the data was compliant with the Common Information Model. Salient CRGT also translated all legacy SIEM rules into Splunk rules and created automated alerts triggered by those rules.

SalientCRGT

SalientCRGT.com

4000 Legato Road • Suite 600 • Fairfax, VA 22033 • 703-891-8200

Salient CRGT Splunk Services

IT Operations Visibility Dashboard (OVD)

Challenge – IT operations and application support teams were burdened with hours of unproductive finger-pointing regarding critical incidents. Each area with its own support teams analyzed only its own problem logs. There was no unified log view that could identify application issues and their causes. Additionally, there was no way of tracking and predicting the volume of transactions hitting the systems at given points in time, leading to service degradation and related problems. The ability to correlate user behavior and performance issues was missing – always a critical need but especially during busy seasons.

Salient CRGT's Approach – Employing Splunk, Salient CRGT developed the OVD, consolidating all machine logs from various tiers together into a single data store, thereby providing a single window into application behavior and traffic not only for IT operations but also for use by the business units. OVD slices data into functional domains, provides analysis on critical incidents, and presents root cause information. Splunk's ability to provide real-time monitoring of system performance, monitor user behavior, create triggered alerts, define trend data, and present a "common language" to users reduced significantly the time and cost of critical incident resolution for our customer.

Salient CRGT's Splunk practice have:

- Continuous innovation through Splunk prototyping to demonstrate data analytic solutions to our customers.
- Labs that are accessible 24x7 to all Splunk practitioners to increase their skills and to develop new applications.
- Availability of Splunk labs to Salient CRGT customers in order to test drive apps and evaluate their applicability to business needs.
- Splunk partnership in order to provide both Splunk services and software to federal customers to address their growing needs to turn data into actionable information and business intelligence.

Fraud Detection

Challenge – Digital fraud, an immense challenge for many online organizations, takes multiple forms: credit card fraud, account take overs, wire transfer fraud, student loan fraud, and many others. Fraud perpetrators constantly change their methods, becoming more sophisticated. Often fraud tools generate many false alarm alerts. Investigating and determining fraud is time consuming and expensive, an unfortunate cost of doing business.

Salient CRGT's Approach – Salient CRGT identifies indicators of cyber-attacks at the time of registrations, logins, and transactions processing. We look for behavior patterns and correlate them with other data points, e.g., known fraud behavior. We use Splunk to identify indicators, patterns and alerts, and the relationships among them. Our capability generates alerts using statistical techniques, comparing captured data with historical "normal" behavior. Normal behavior is defined within dynamic control limits; outlier data identifies anomalous behavior for further investigation to determine fraudulent activity. Salient CRGT's dynamic controls, based upon historical patterns and multi-variate analysis (aggregating multiple fraud scores), result in reduced false alarms, lowering the cost and increasing the accuracy of fraud detection and investigation.

A Partnership that Benefits You

Whether you require sophisticated data analytics in support of your business objectives, predictive analysis in order to identify application issues before they impact your customers' experience, or the identification of potential security risks, Salient CRGT and Splunk can provide you with the data management and analytics thought leadership to help you achieve your business objectives. Let us show you how we can quickly put our partnership to work for you.

SalientCRGT

SalientCRGT.com
4000 Legato Road • Suite 600 • Fairfax, VA 22033 • 703-891-8200