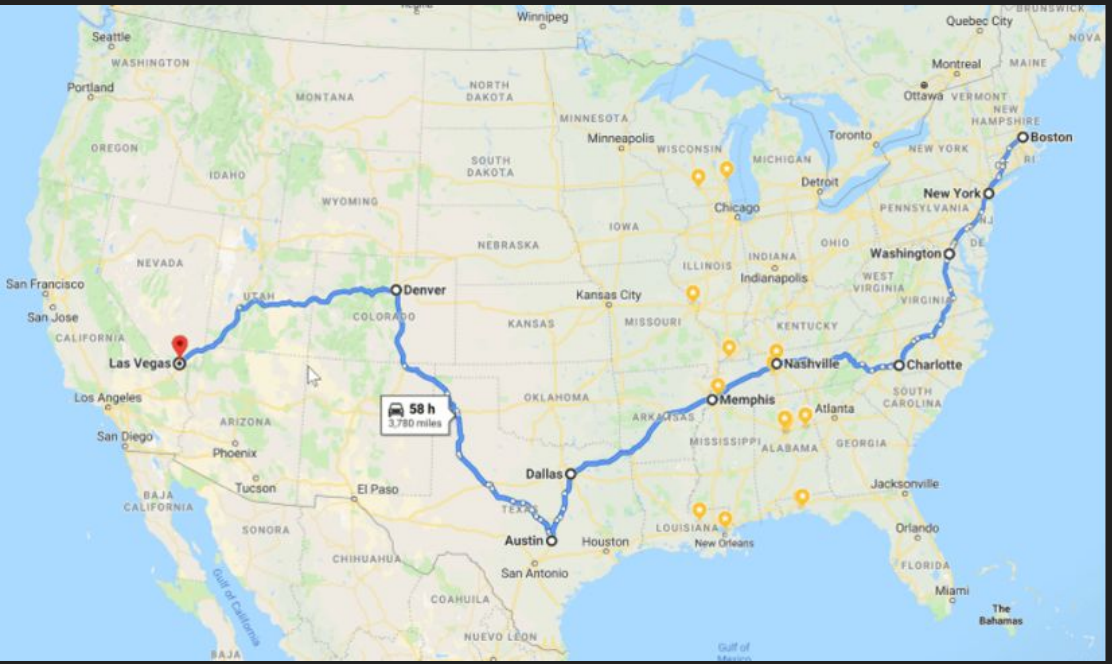
Conf19 Recap

What's New!

NEW Colors!

BigDataBeard RV Road to Splunk .Conf19 Trip



7 OCTOBER 2019
BOSTON, MA

7 OCTOBER 2019
NEW YORK, NY

8 OCTOBER 2019
WASHINGTON, D.C.

9 OCTOBER 2019
CHARLOTTE, NC

10-11 OCTOBER 2019
NASHVILLE, TN

12 OCTOBER 2019
MEMPHIS, TN

BIG DATA
www.BigDataBeard.com

13 OCTOBER 2019
DALLAS, TX

14-15 OCTOBER 2019
AUSTIN, TX

16 OCTOBER 2019
AMARILLO, TX

17 OCTOBER 2019
DENVER, CO

18 OCTOBER 2019
BOULDER, CO

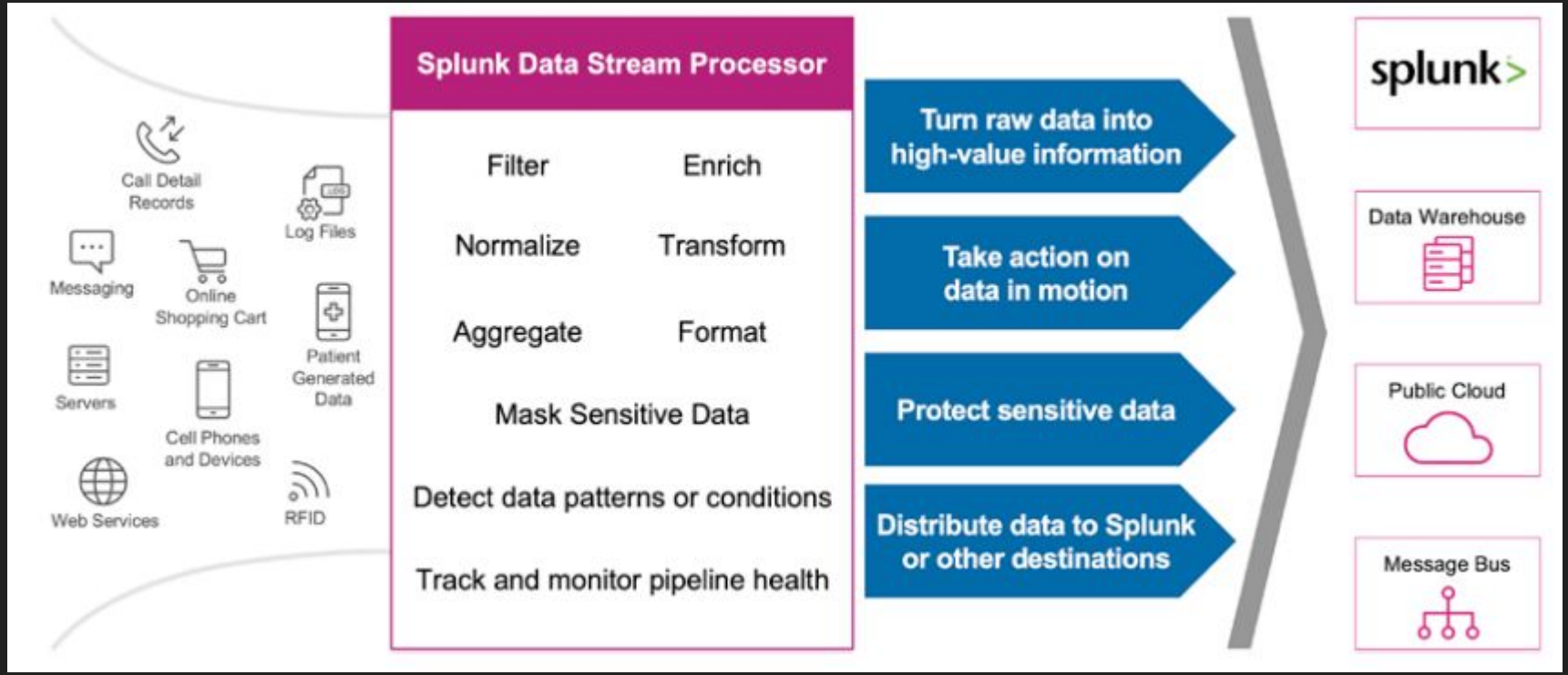
19-25 OCTOBER 2019
LAS VEGAS, NV

Splunk Enterprise 8.0

- Python 3.7 Support (just in time for python 3.8</snarc>)
- Improvements to Workload management
- Analytics Workspace
- Search / Metric Performance and Storage Improvements
- Ability to share data model acceleration summaries across search heads (finally)
- Improvements to Health Checks and monitoring
- Search Bundle Peer based replication
- New Role management UI and improvements with managing restricted search filters

Data Stream Processor

Officially GA



Splunk Cloud

- Of course Upgraded to 8.0
- Officially FedRamp Certified
- Moderate impact level authorization

Natural Language Platform

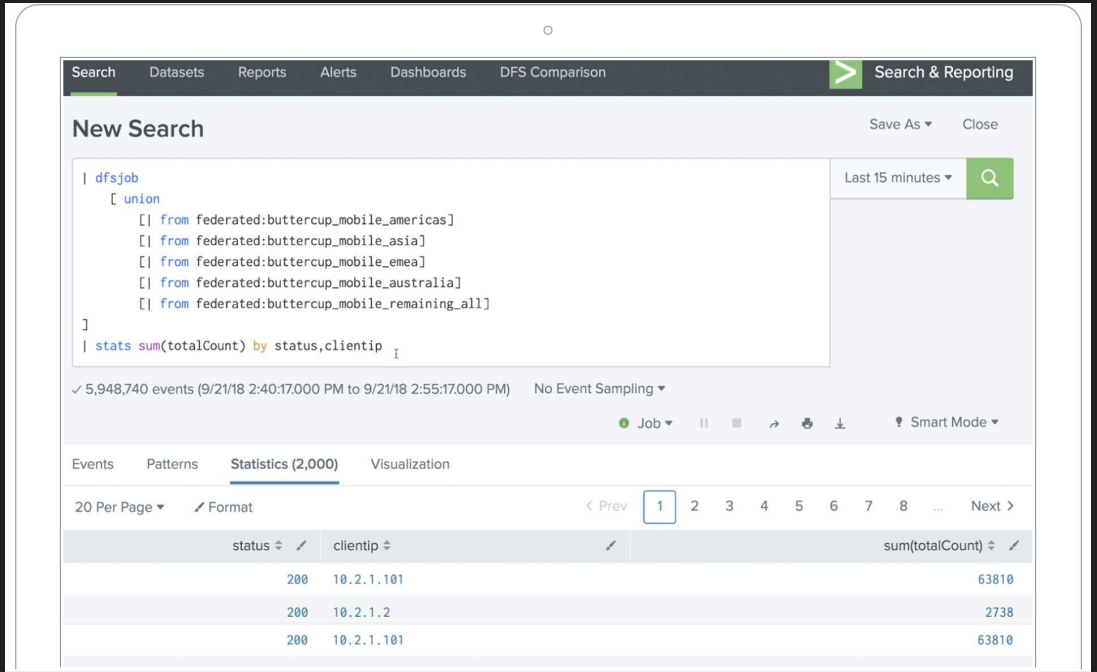
- Officially GA
- Supported on SplunkTV and iOS Splunk Mobile
- Android coming soon
- Allows users to use voice to ask splunk questions or change views
- Requires Cloud Gateway
- Requires pre-learned intent taxonomy

Splunk Connected Experience

- Requires Splunk Cloud Gateway
  - Supports SAML in Splunk 8.0
- Mobile - iOS and Android GA
  - Phantom support - iOS only
- AR - iOS only
  - Now supports rich media in an AR Experience (videos/documents)
- SplunkTV - Apple TV
  - Support for new Dashboards coming to SplunkTV soon…

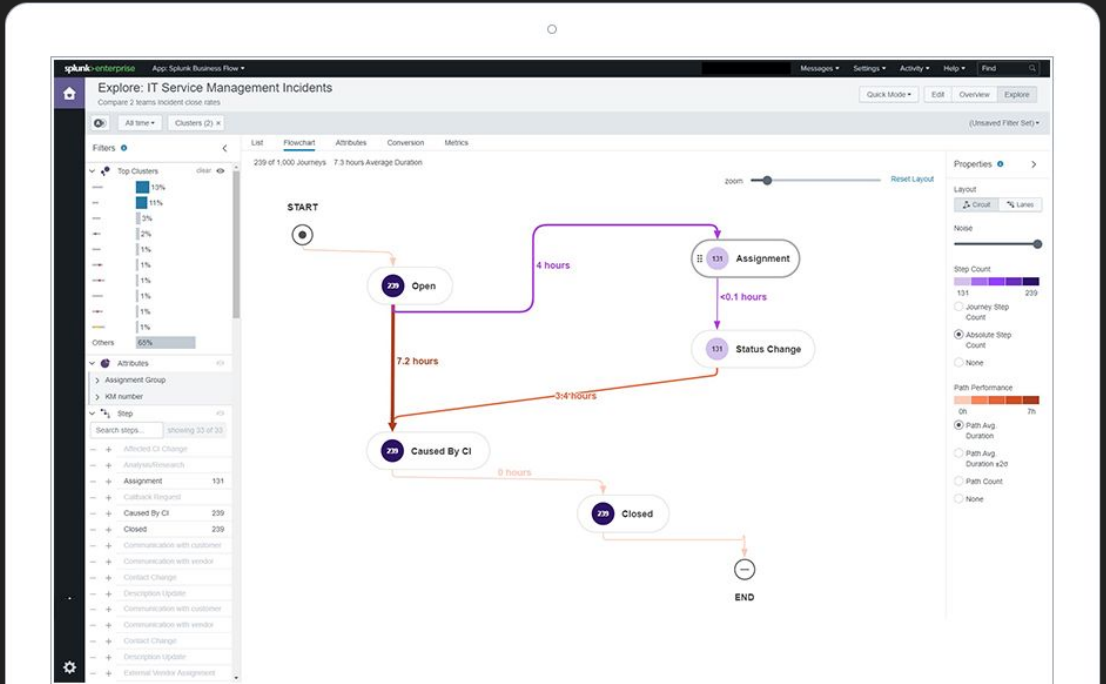
Data Fabric Search

- Federate Search Across many splunk deployments
- Search third-party data stores (Pre-Release)



Splunk Business Flow

- Now GA
- Allows several events to be correlated into a business function
- Better represent the events in a business process
- New UI for analysis



IT Service Intelligence 4.4

- Python 3 Support
- Content Packs (Similar to Enterprise Security)
- Improved Backup/Restore
- VMWare monitoring
- New glass table editor

Enterprise Security 6.0

- With the release of ES 6.0 and the passage of 24 months from the major release, ES 4.x has reached the end of support. The 6.0 version of ES supports upgrading from version 4.7.6 or later.
- Partial Python3 support
- RIP Extreme Search
- KV Store to replace legacy lookup asset & identities
  - Support for new custom fields
  - add up to 20 custom fields for your lookups. Key fields are non editable, such as identity

User Behavior Analytics 5.0

- Improvement in DR/ Backup / Failover
- New HR data fields
- Improved SSO
- Custom Models and UBA use cases

Splunk App for Infrastructure 2.0

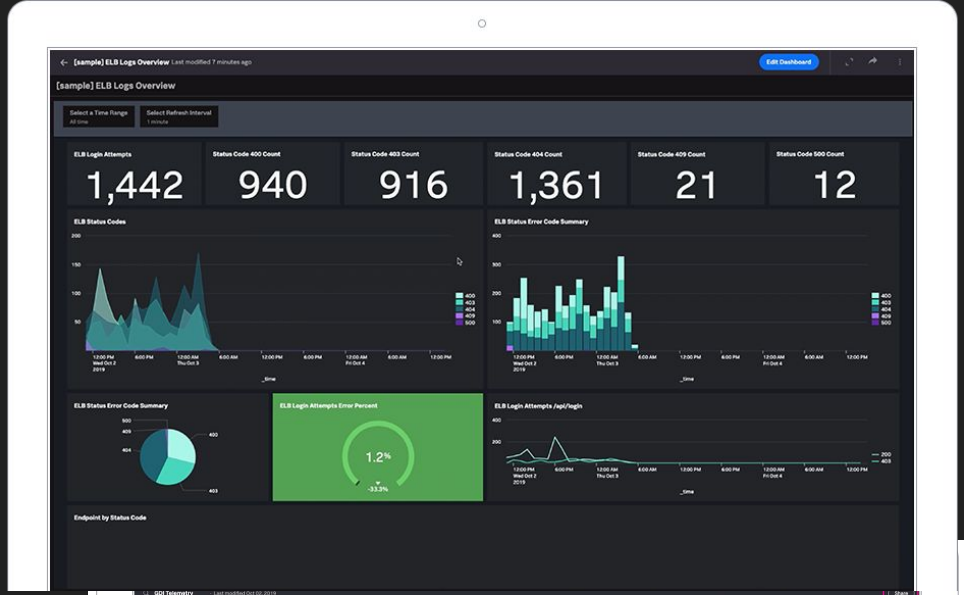
- Python 3
- VMWare Collection -Requires ITSI
- Linux/Windows Process Monitoring
- Slack Alert Actions - Built in
- Debian/Ubuntu support
- Alerts run as “Nobody” -- Security risk?
- Splunk Telemetry for more splunk snooping
-

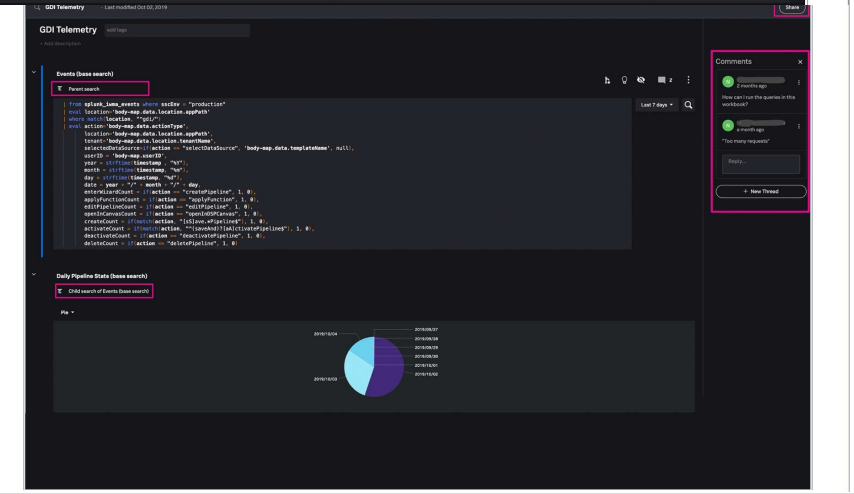
Machine Learning Toolkit 5.0

- Python 3 Required
- Built in Smart Outlier Detection Assistant
- New Algorithms and Scoring Methods
- Additional algorithms available on github
- Support for the new Splunk MLTK Container for TensorFlow™
    - Allowing you to support GPU hardware for offloaded deep learning activities

Splunk Investigate

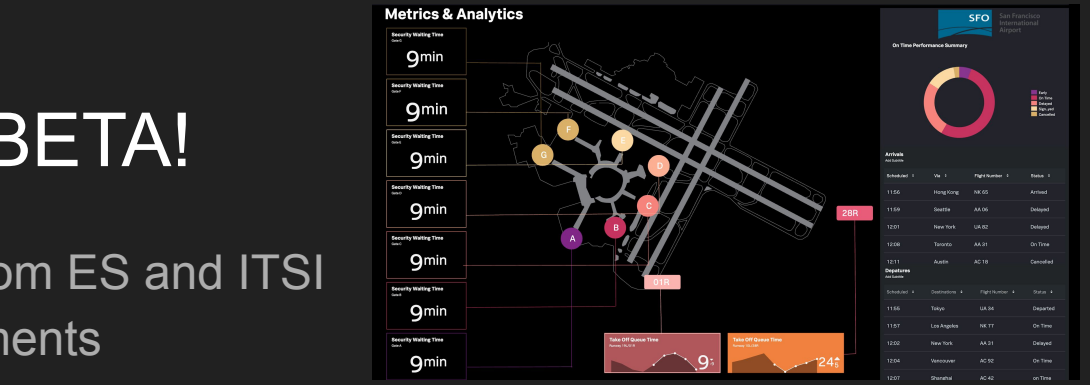
- Cloud Native UI for dashboarding and searching
- Collaborate and review incidents
- Use SQL like language to search data





Splunk Dashboards - BETA!

- An evolution of glass tables from ES and ITSI
- Easy drag drop and align elements
- Available for 7.3 and 8.0
- On Splunkbase

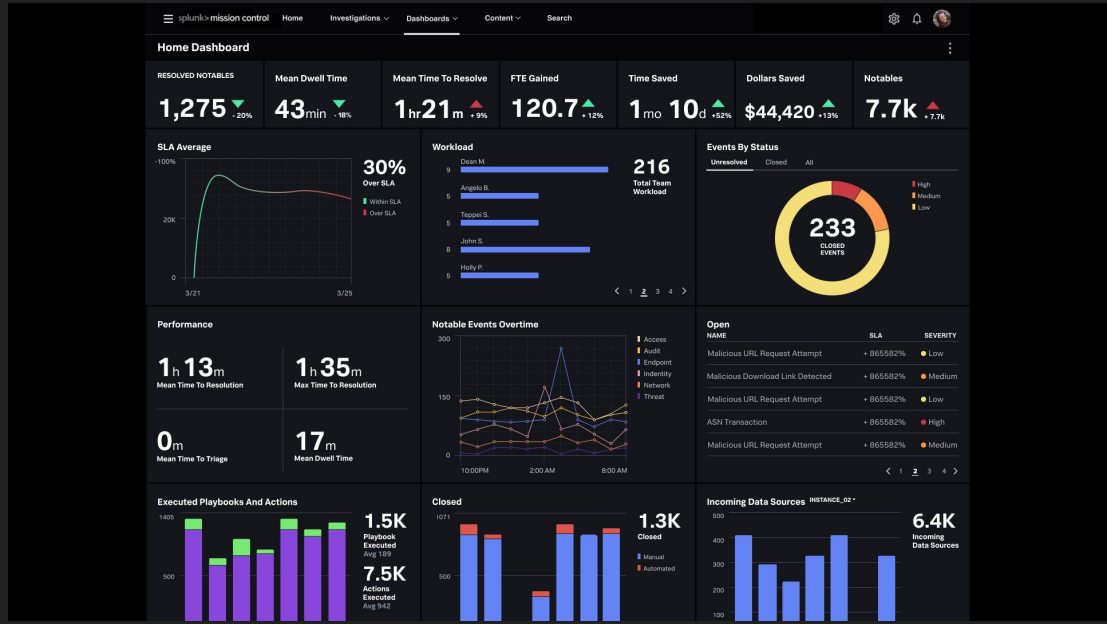


Splunk Virtual Reality (VR) Beta!

- Leveraging Unity they created a 3d world overlaid with splunk dashboards
- Even created collaborative multi user experience to work on a problem

Mission Control (Beta?)

A unified experience that modernizes and optimizes your team's security operations. The cloud-based software-as-a-service (SaaS) allows you to detect, manage, investigate, hunt, contain, and remediate threats and other high-priority security issues across the entire event lifecycle—all from the common work surface it provides.



Slack!

spk.it/slack #ug_baltimore