splunk> .conf2017

Using Datasets

Easier Data Exploration, Preparation and Analysis

Jesse Miller | Staff Sales Engineer
Megumi Hora | Software Engineer

September 2017 | Washington, DC

Forward-Looking Statements

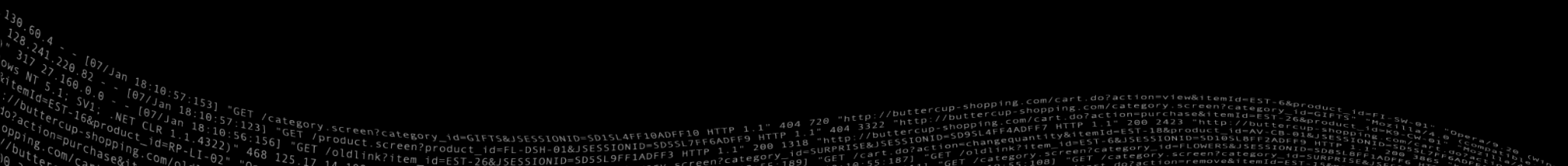
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk> .conf2017

Agenda

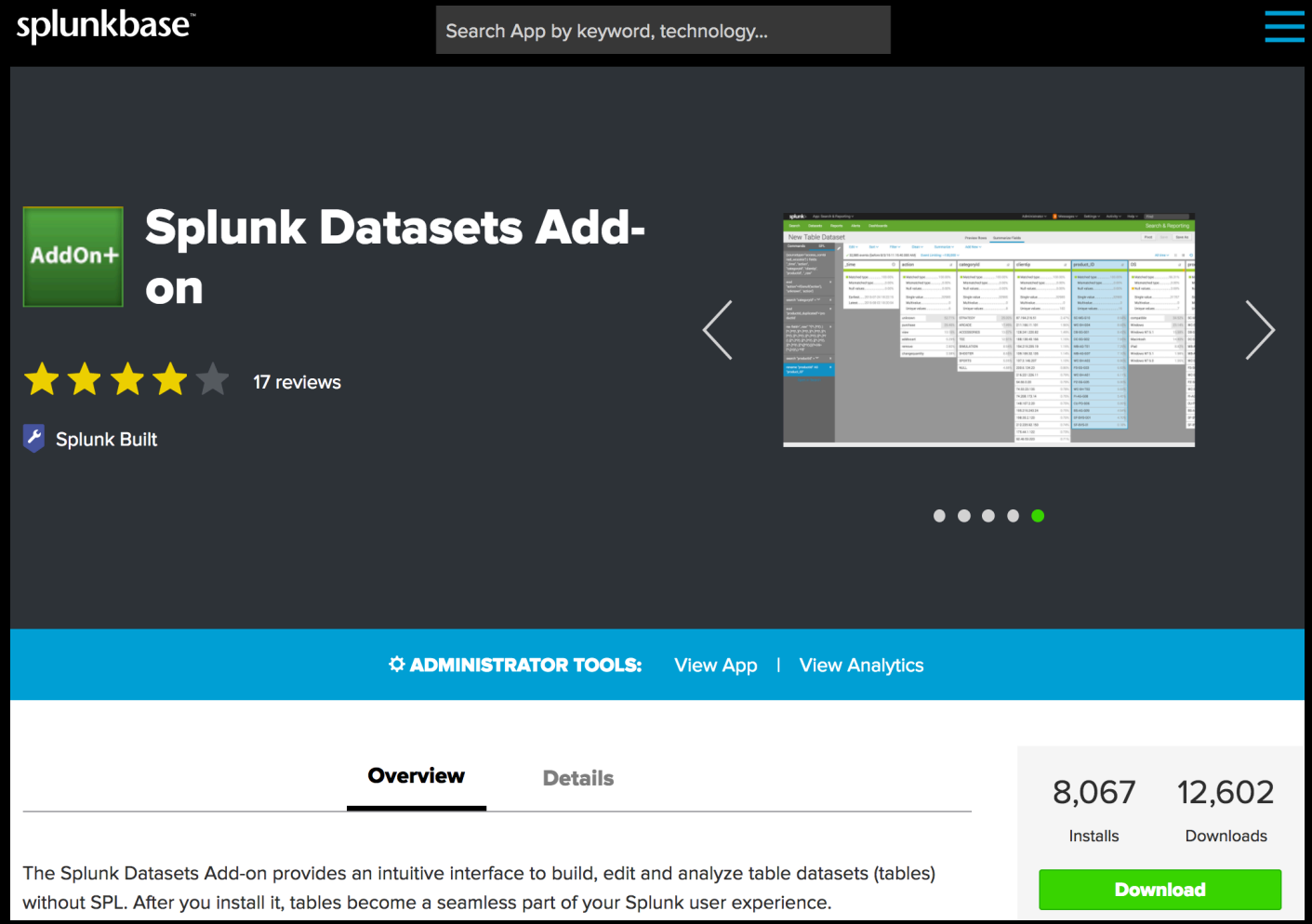
- What are Datasets?
- Types of Datasets
- Using Datasets
- Datasets: Listing, Viewing, Editing
- Demo
- Questions



splunk> .conf2017

What Are Datasets?

- **Building Blocks**
  - Source Data
  - SPL
  - Schema
- **Unified Endpoint**
  - List
  - View
  - Search
  - Edit
  - Analyze



Types Of Datasets

Lookups

- **What**: Static data (CSV)
  Dynamic data (Script)
  DBConnect (SQL)
- **Why**: Enrich search-based datasets by adding fields from external sources
- **Where:** Lookups
  Transforms.conf

Data Model (Objects)

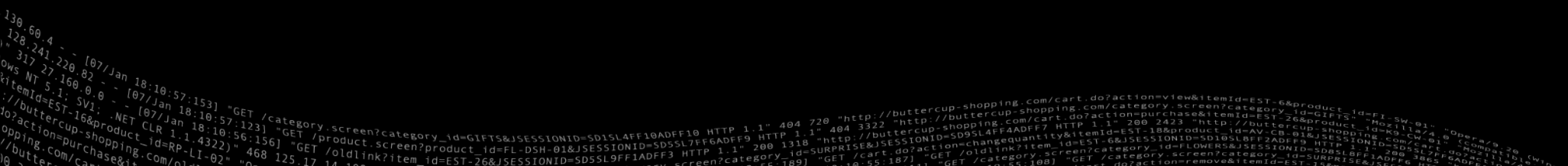
- **What**: search-based datasets with a hierarchical structure, grouped as "Data Models".
- **Why:** Establishing hierarchical relationships with domain knowledge. (top-down)
- **Where:** Data Model Editor
  Datasets.conf (JSON)

Tables*

New!

- **What:** Tabular, search-based dataset (similar to the individual objects in a DM)
- **Why:** Agile creation and iterative refinement.
  (bottom-up)
- **Where:** Table Editor*
  Datamodels.conf (JSON)

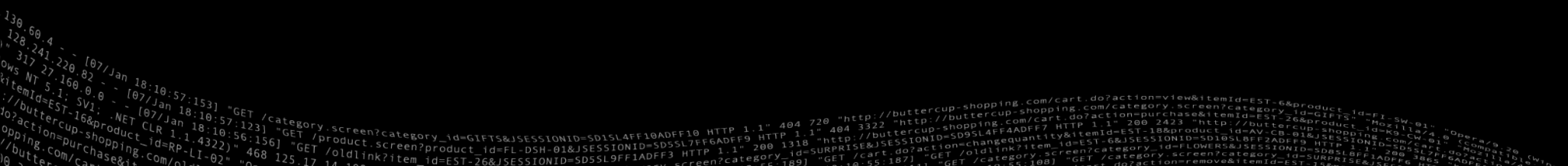
* Available with the Tables Add-On (Table Datasets)



splunk> .conf2017

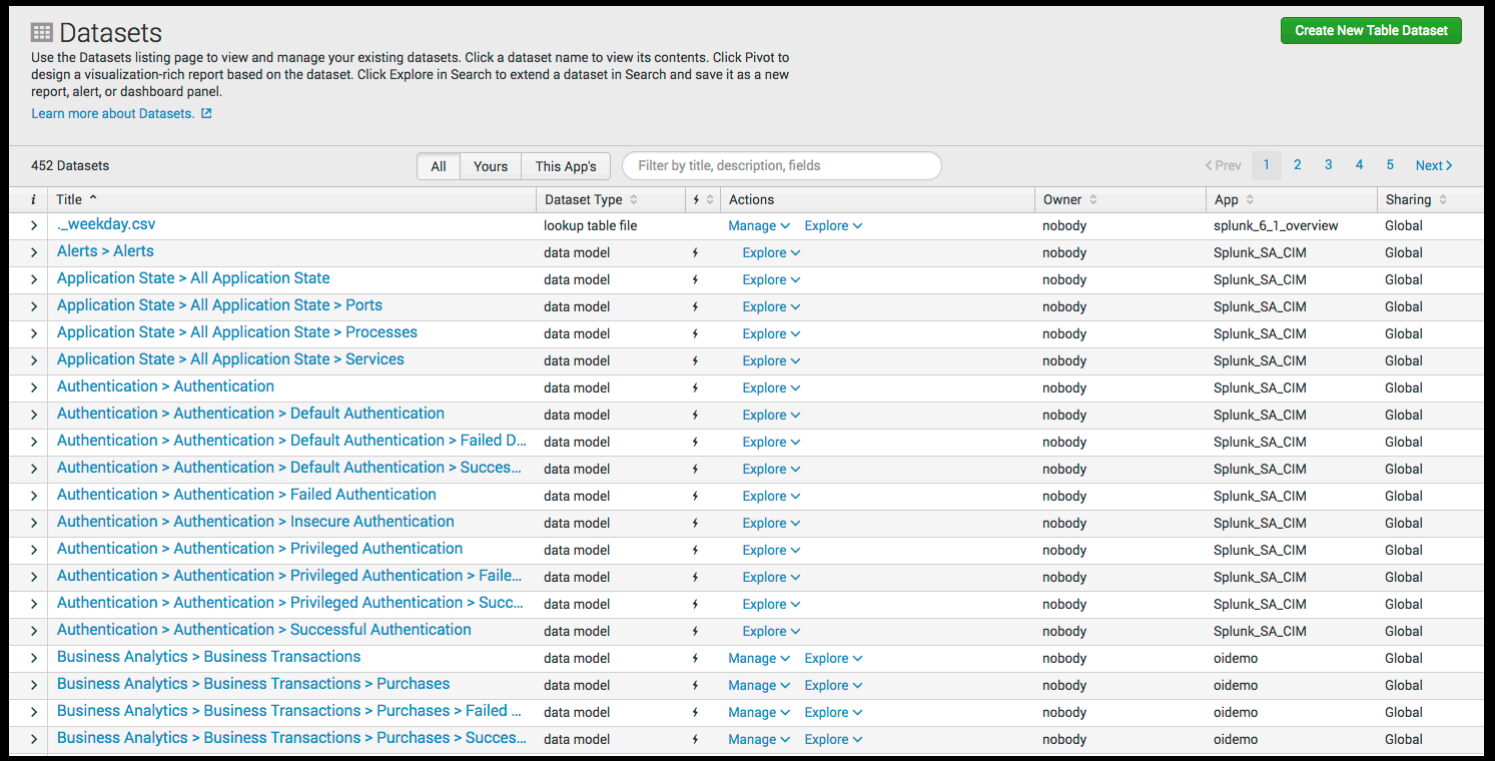
Using Datasets

- Datasets can be extended, forming a parent/child model of inheritance
- Datasets can be queried
  - | *from type:"name"* | *eval ...* | *search ...* | *stats ...*
- Datasets can be accelerated
- Datasets can be pivoted
- Datasets can be data model objects



Datasets: Listing

- Manage table datasets, data model datasets, and lookups in one place
- Define acceleration and permissions
- Search for datasets based on name and contained fields



Datasets

Use the Datasets listing page to view and manage your existing datasets. Click a dataset name to view its contents. Click Pivot to design a visualization-rich report based on the dataset. Click Explore in Search to extend a dataset in Search and save it as a new report, alert, or dashboard panel.

Learn more about Datasets.

Create New Table Dataset

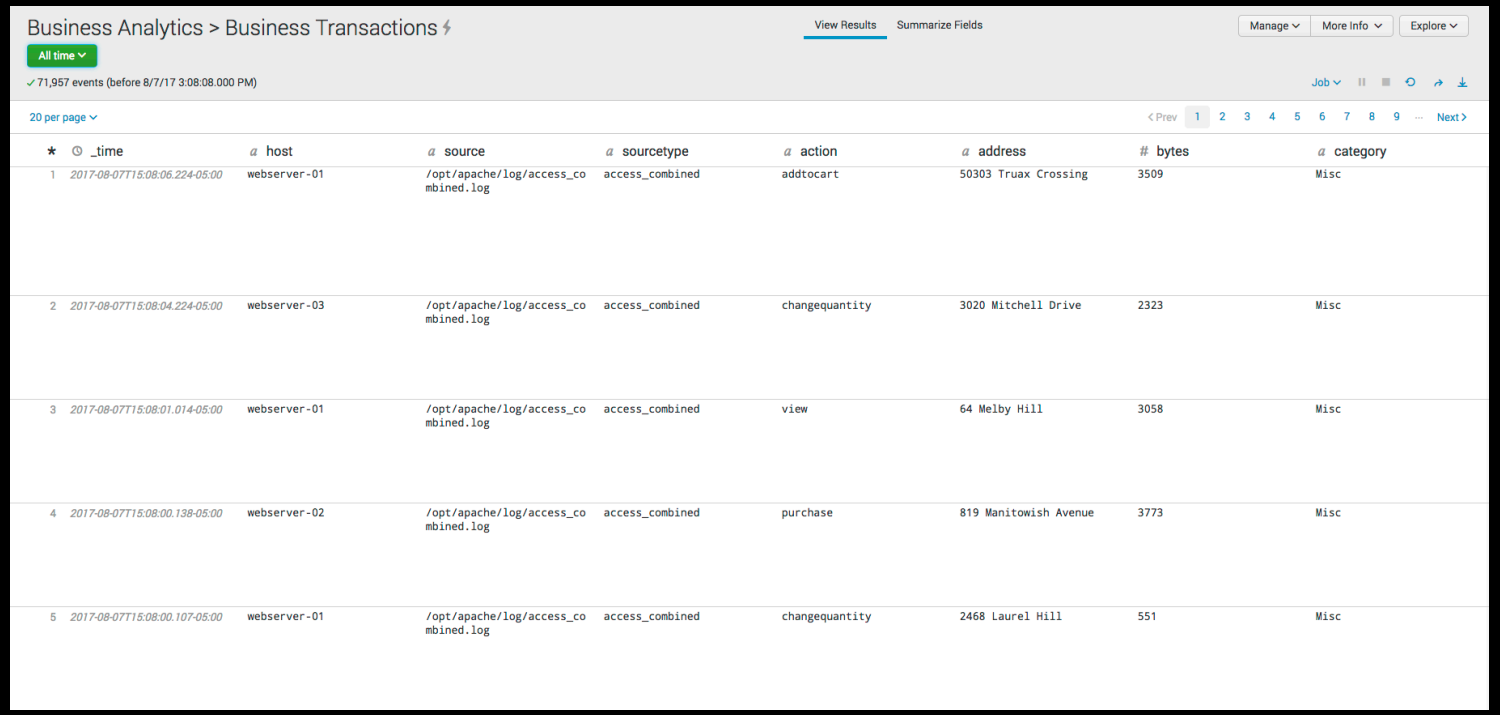
452 Datasets | All | Yours | This App's | Filter by title, description, fields | < Prev 1 2 3 4 5 Next >

Title	Dataset Type	Actions	Owner	App	Sharing
._weekday.csv	lookup table file	Manage Explore	nobody	splunk_6_1_overview	Global
Alerts > Alerts	data model	Explore	nobody	Splunk_SA_CIM	Global
Application State > All Application State	data model	Explore	nobody	Splunk_SA_CIM	Global
Application State > All Application State > Ports	data model	Explore	nobody	Splunk_SA_CIM	Global
Application State > All Application State > Processes	data model	Explore	nobody	Splunk_SA_CIM	Global
Application State > All Application State > Services	data model	Explore	nobody	Splunk_SA_CIM	Global
Authentication > Authentication	data model	Explore	nobody	Splunk_SA_CIM	Global
Authentication > Authentication > Default Authentication	data model	Explore	nobody	Splunk_SA_CIM	Global
Authentication > Authentication > Default Authentication > Failed D...	data model	Explore	nobody	Splunk_SA_CIM	Global
Authentication > Authentication > Default Authentication > Succes...	data model	Explore	nobody	Splunk_SA_CIM	Global
Authentication > Authentication > Failed Authentication	data model	Explore	nobody	Splunk_SA_CIM	Global
Authentication > Authentication > Insecure Authentication	data model	Explore	nobody	Splunk_SA_CIM	Global
Authentication > Authentication > Privileged Authentication	data model	Explore	nobody	Splunk_SA_CIM	Global
Authentication > Authentication > Privileged Authentication > Faile...	data model	Explore	nobody	Splunk_SA_CIM	Global
Authentication > Authentication > Privileged Authentication > Succ...	data model	Explore	nobody	Splunk_SA_CIM	Global
Authentication > Authentication > Successful Authentication	data model	Explore	nobody	Splunk_SA_CIM	Global
Business Analytics > Business Transactions	data model	Manage Explore	nobody	oidemo	Global
Business Analytics > Business Transactions > Purchases	data model	Manage Explore	nobody	oidemo	Global
Business Analytics > Business Transactions > Purchases > Failed ...	data model	Manage Explore	nobody	oidemo	Global
Business Analytics > Business Transactions > Purchases > Succes...	data model	Manage Explore	nobody	oidemo	Global

splunk> .conf2017

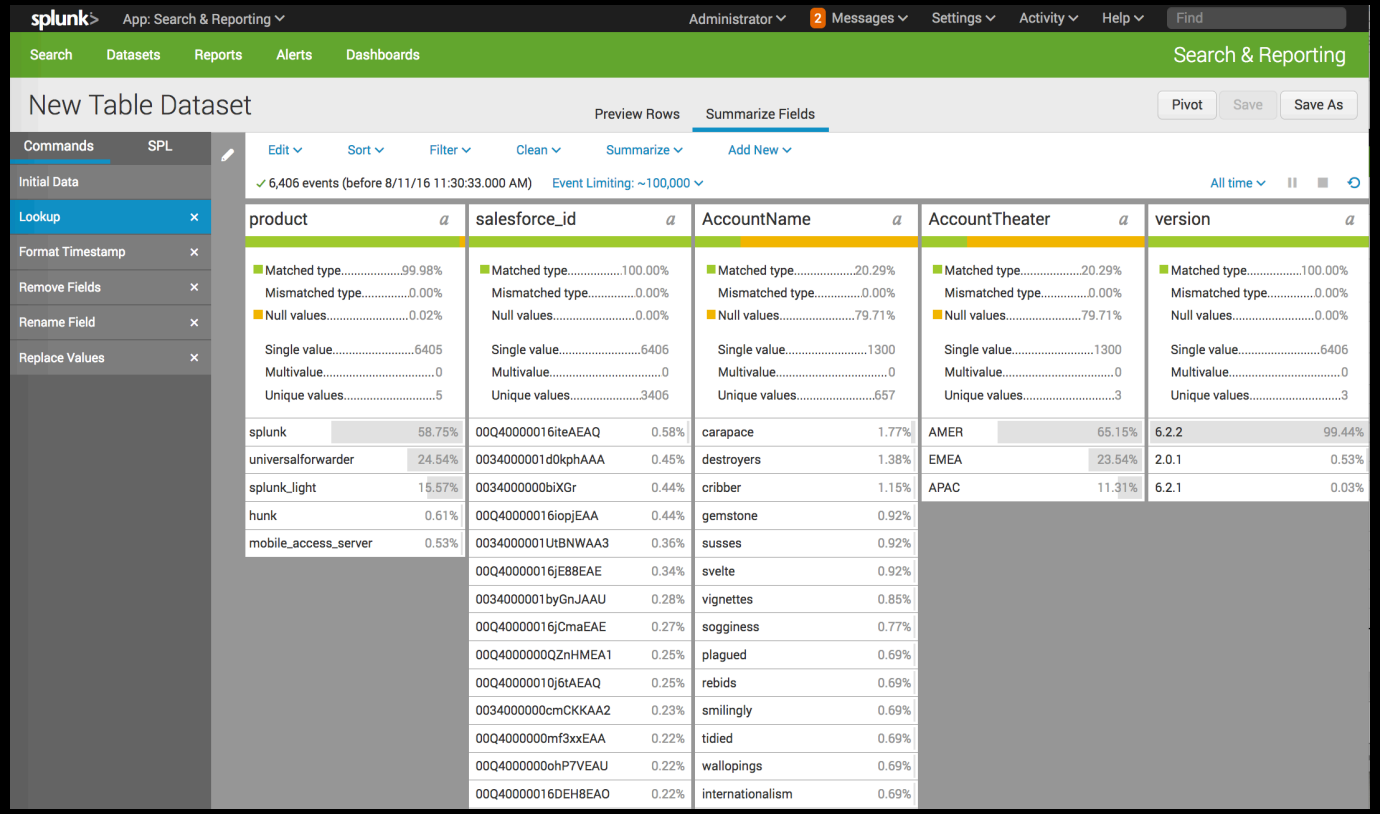
Datasets: Viewing

- Explore existing dataset
- Two views (read only):
  - Preview Rows (table)
  - Summarize Fields (field stats)
- Filter data by time range
- Manage dataset search jobs

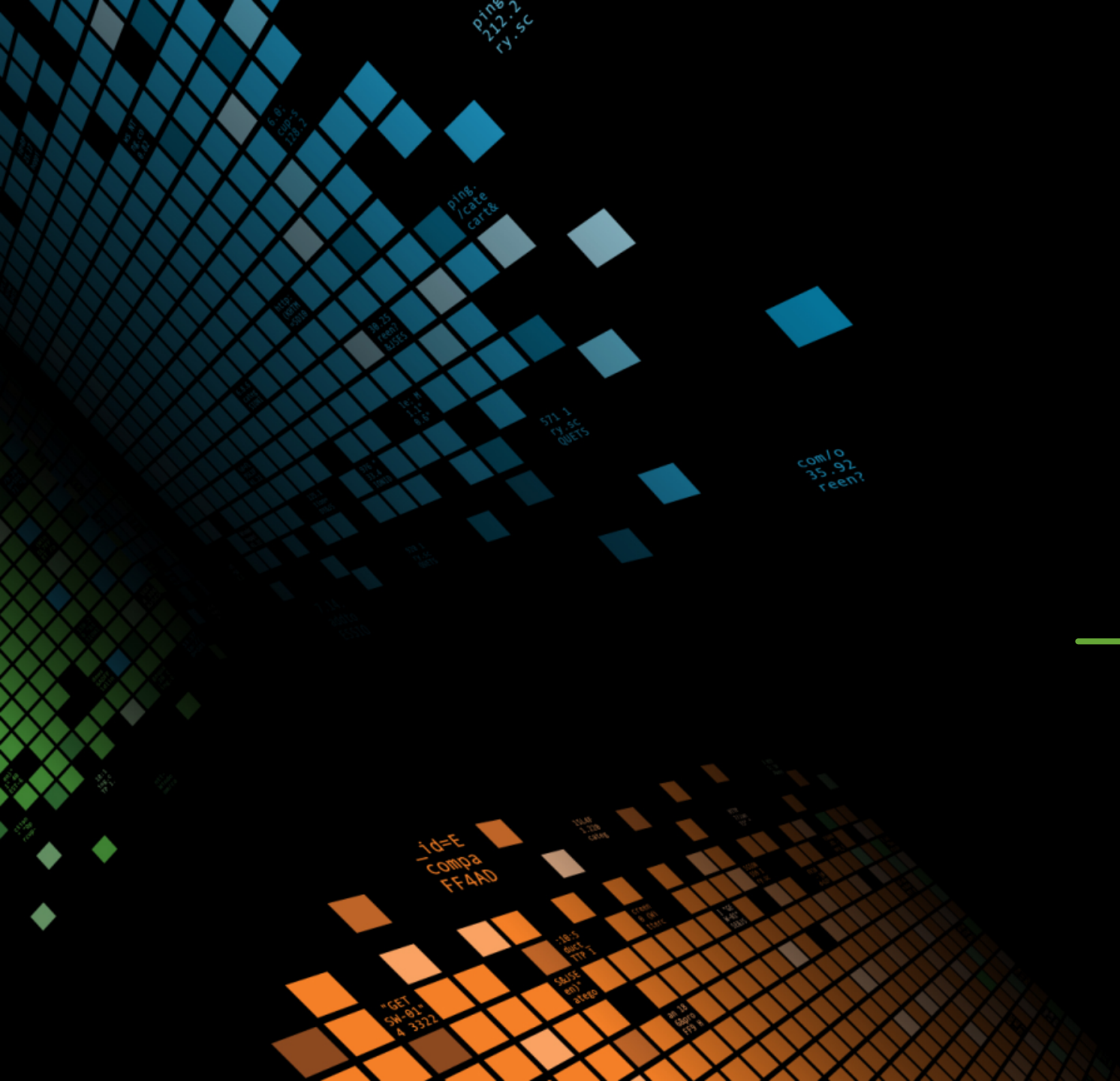


Datasets: Table Editor

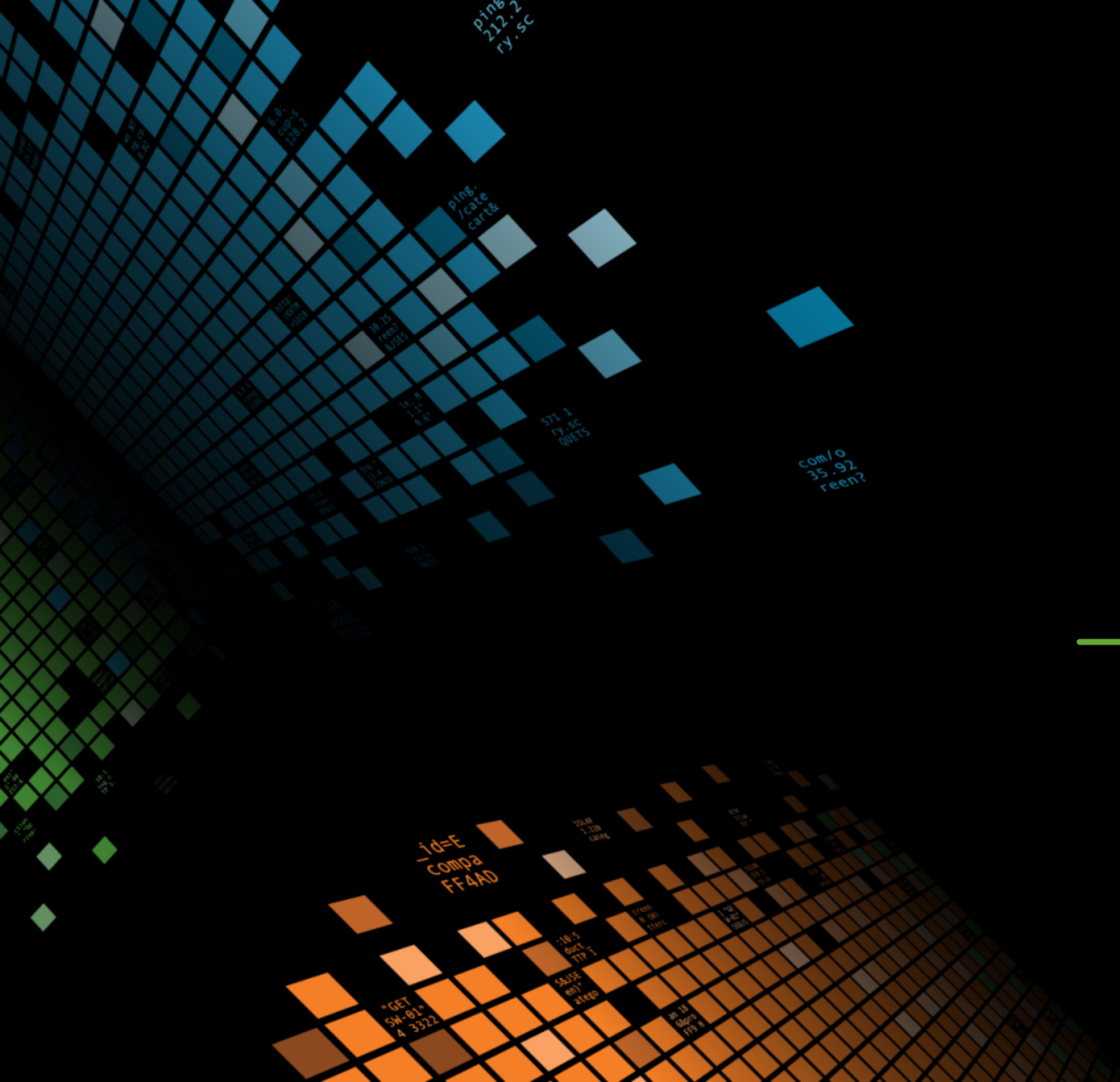
- Refine dataset with SPL commands using selections, menus, and forms
- Two views:
  - Preview Rows (table)
  - Summarize Fields (field stats)
- Command history
- Field types



Demo



Q&A



Thank You!

splunk> .conf2017

Thank You

Don't forget to rate this session in the .conf2017 mobile app