APRIL 13, 2017 | SAN FRANCISCO, CA

splunk> live!

APRIL 13, 2017 | SAN FRANCISCO, CA

Power of Splunk
Search Processing Language (SPL™)

Stephen Luedtke | Sr. Technical Product Marketing Manager

Safe Harbor Statement

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>live!

Agenda

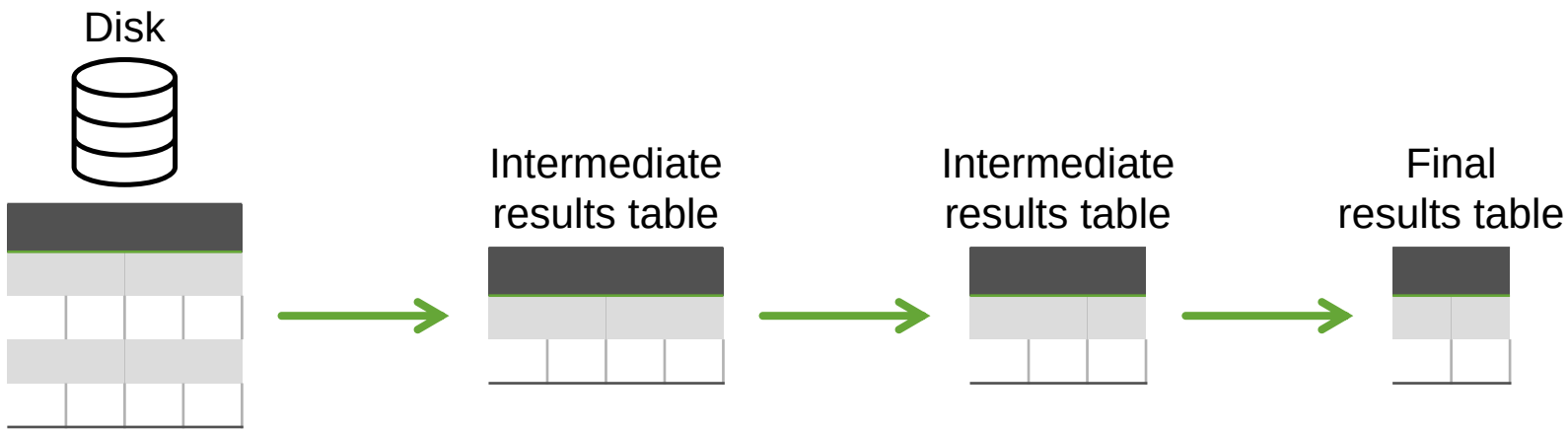
1. Overview & Anatomy of a Search
   - Quick refresher on search language and structure
2. SPL Commands and Examples
   - Searching, charting, converging, mapping, transactions, anomalies, exploring
3. Custom Commands
   - Extend the capabilities of SPL
4. Q&A

SPL Overview

splunk>live!

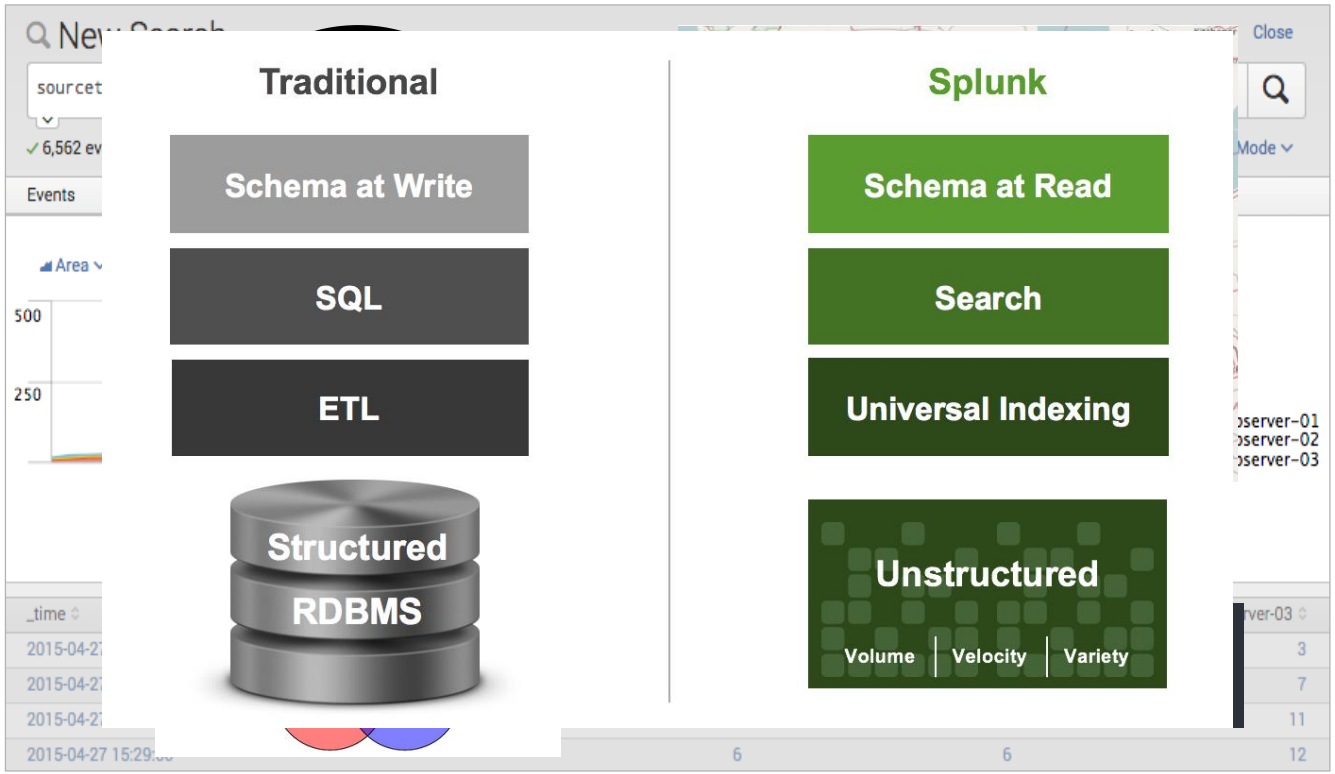
SPL Overview

- Over 140 search commands
- Syntax was originally based upon the **Unix pipeline** and SQL and is optimized **for time-series data**
- The scope of SPL includes data searching, filtering, modification, manipulation, enrichment, insertion and deletion
- Includes machine learning such as anomaly detection



Why Create a New Query Language?

- Flexibility and effectiveness on *small* and ***big*** data
- Late-binding schema
- More/better methods of correlation
- Not just analyze, but visualize



SPL Basic Structure

search and filter | munge | report | cleanup

```
sourcetype=access*
| eval KB=bytes/1024
| stats sum(KB) dc(clientip)
| rename sum(KB) AS "Total KB" dc(clientip) AS "Unique Customers"
```

SPL Examples

splunk>live!

SPL Examples and Recipes

- Find the needle in the haystack
- Charting statistics and predicting values
- Enriching and converging data sources
- Map geographic data in real time
- Identifying anomalies
- Transactions
- Data exploration & finding relationships between fields
- Custom commands

splunk>live!

SPL Examples and Recipes

- **Find the needle in the haystack**
- Charting statistics and predicting values
- Enriching and converging data sources
- Map geographic data in real time
- Identifying anomalies
- Transactions
- Data exploration & finding relationships between fields
- Custom Commands

splunk>live!

Eval – Just Getting Started!

Splunk Search Quick Reference Guide

Common Eval Functions	The eval command calculates an expression and puts the resulting value into a field (e.g. "...| eval force = mass * acceleration"). The following table lists some of the functions used with the eval command. You can also use basic arithmetic operators (+ - * / %), string concatenation (e.g., "...| eval name = last . "," . first"), and Boolean operations (AND OR NOT XOR < > <= >= != = == LIKE).

Function	Description	Examples
abs(X)	Returns the absolute value of X.	abs(number)
case(X,"Y",…)	Takes pairs of arguments X and Y, where X arguments are Boolean expressions. When evaluated to TRUE, the arguments return the corresponding Y argument.	case(error == 404, "Not found", error == 500,"Internal Server Error", error == 200, "OK")
ceil(X)	Ceiling of a number X.	ceil(1.9)
cidrmatch("X",Y)	Identifies IP addresses that belong to a particular subnet.	cidrmatch("123.132.32.0/25",ip)
coalesce(X,…)	Returns the first value that is not null.	coalesce(null(), "Returned val", null())
cos(X)	Calculates the cosine of X.	n=cos(0)
exact(X)	Evaluates an expression X using double precision floating point arithmetic.	exact(3.14*num)
exp(X)	Returns eX.	exp(3)
if(X,Y,Z)	If X evaluates to TRUE, the result is the second argument Y. If X evaluates to FALSE, the result evaluates to the third argument Z.	if(error==200, "OK", "Error")
isbool(X)	Returns TRUE if X is Boolean.	isbool(field)
isint(X)	Returns TRUE if X is an integer.	isint(field)
isnull(X)	Returns TRUE if X is NULL.	isnull(field)
isstr()	Returns TRUE if X is a string.	isstr(field)
len(X)	This function returns the character length of a string X.	len(field)
like(X,"Y")	Returns TRUE if and only if X is like the SQLite pattern in Y.	like(field, "addr%")

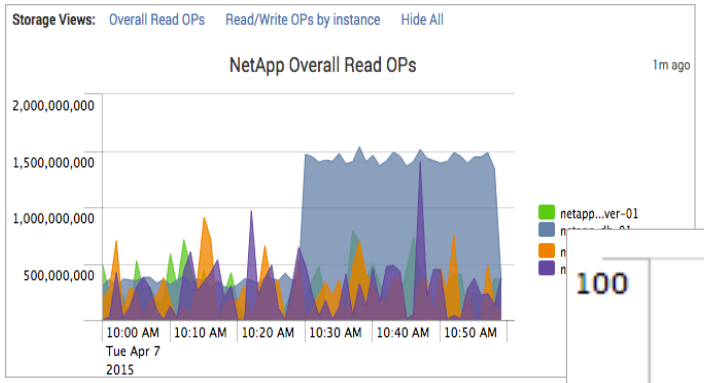
splunk>live!

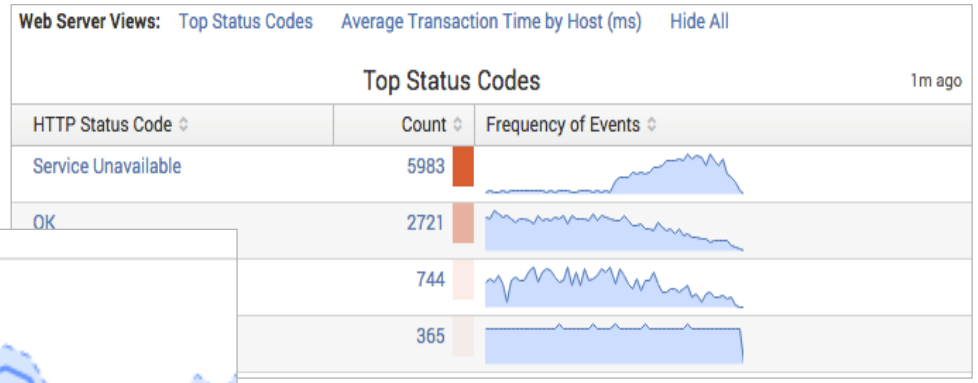
SPL Examples and Recipes

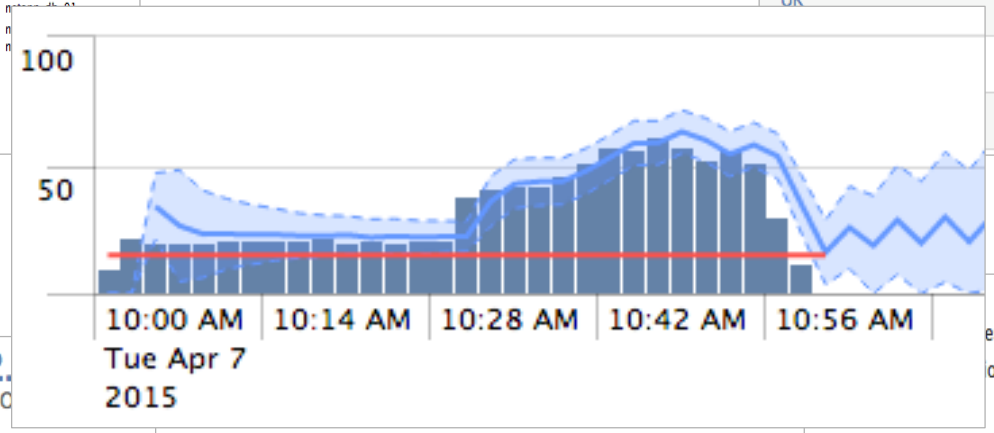
- Find the needle in the haystack
- **Charting statistics and predicting values**
- Enriching and converging data sources
- Map geographic data in real time
- Identifying anomalies
- Transactions
- Data exploration & finding relationships between fields
- Custom commands

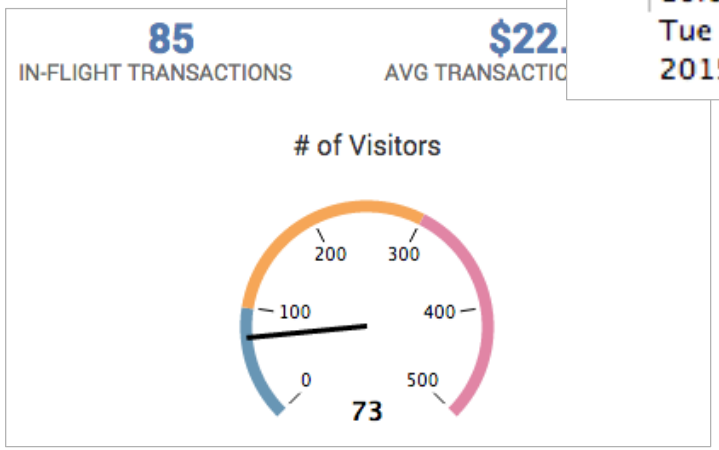
splunk>live!

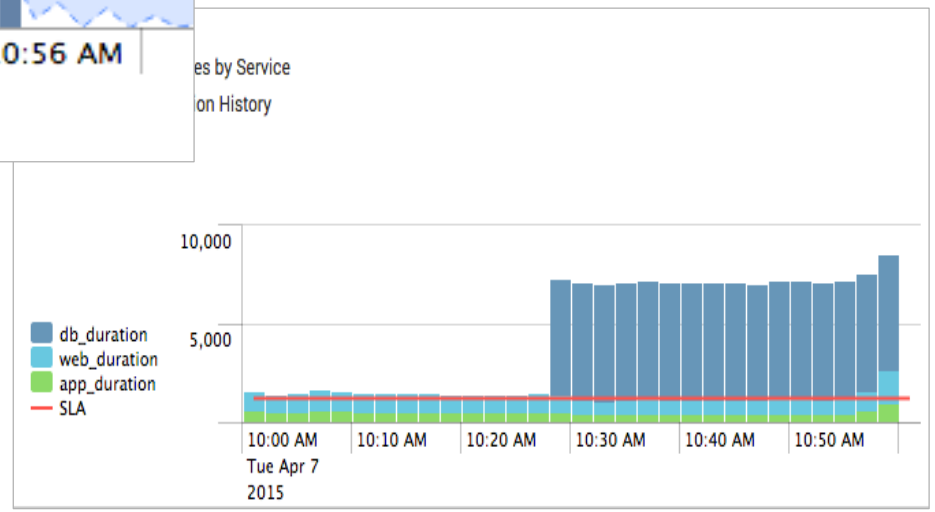
Stats, Timechart, Eventstats, Streamstats











splunk>live!

Stats/Timechart – But Wait, There's More!

Splunk Search Quick Reference Guide

Common Stats Functions	Common statistical functions used with the chart, stats, and timechart commands. Field names can be wildcarded, so avg(*delay) might calculate the average of the delay and xdelay fields.
avg(X)	Returns the average of the values of field X.
count(X)	Returns the number of occurrences of the field X. To indicate a specific field value to match, format X as eval(field="value").
dc(X)	Returns the count of distinct values of the field X.
earliest(X)	Returns the chronologically earliest seen value of X.
latest(X)	Returns the chronologically latest seen value of X.
max(X)	Returns the maximum value of the field X. If the values of X are non-numeric, the max is found from alphabetical ordering.
median(X)	Returns the middle-most value of the field X.
min(X)	Returns the minimum value of the field X. If the values of X are non-numeric, the min is found from alphabetical ordering.
mode(X)	Returns the most frequent value of the field X.
perc<X>(Y)	Returns the X-th percentile value of the field Y. For example, perc5(total) returns the 5th percentile value of a field "total".
range(X)	Returns the difference between the max and min values of the field X.
stdev(X)	Returns the sample standard deviation of the field X.
stdevp(X)	Returns the population standard deviation of the field X.
sum(X)	Returns the sum of the values of the field X.
sumsq(X)	Returns the sum of the squares of the values of the field X.
values(X)	Returns the list of all distinct values of the field X as a multi-value entry. The order of the values is alphabetical.
var(X)	Returns the sample variance of the field X.

splunk>live!

SPL Examples and Recipes

- Find the needle in the haystack
- Charting statistics and predicting values
- **Enriching and converging data sources**
- Map geographic data in real time
- Identifying anomalies
- Transactions
- Data exploration & finding relationships between fields
- Custom commands

splunk>live!

Converging Data Sources

Index Untapped Data: Any Source, Type, Volume

splunk>

Ask Any Question

- Application Delivery
- IT Operations
- Security, Compliance and Fraud
- Business Analytics
- Industrial Data and the Internet of Things

splunk>live!

SPL Examples and Recipes

- Find the needle in the haystack
- Charting statistics and predicting values
- Enriching and converging data sources
- **Map geographic data in real time**
- Identifying anomalies
- Transactions
- Data exploration & finding relationships between fields
- Custom commands

splunk>live!

SPL Examples and Recipes

- Find the needle in the haystack
- Charting statistics and predicting values
- Enriching and converging data sources
- Map geographic data in real time
- **Identifying anomalies**
- Transactions
- Data exploration & finding relationships between fields
- Custom commands

splunk>live!

SPL Examples and Recipes

- Find the needle in the haystack
- Charting statistics and predicting values
- Enriching and converging data sources
- Map geographic data in real time
- Identifying anomalies
- **Transactions**
- Data exploration & finding relationships between fields
- Custom commands

splunk>live!

SPL Examples and Recipes

- Find the needle in the haystack
- Charting statistics and predicting values
- Enriching and converging data sources
- Map geographic data in real time
- Identifying anomalies
- Transactions
- **Data exploration & finding relationships between fields**
- Custom commands

splunk>live!

Data Exploration

- | analyzefields
- | anomalies
- | arules
- | associate
- | cluster
- | contingency
- | correlate
- | fieldsummary

SPL Examples and Recipes

- Find the needle in the haystack
- Charting statistics and predicting values
- Enriching and converging data sources
- Map geographic data in real time
- Identifying anomalies
- Transactions
- Data exploration & finding relationships between fields
- **Custom commands**

splunk>live!

Custom Commands

- What is a Custom Command?
  - “| **haversine** origin="47.62,-122.34" outputField=dist lat lon”
- Why do we use Custom Commands?
  - Run other/external algorithms on your Splunk data
  - Save time munging data (see Timewrap!)
  - Because you can!
- Create your own or download as Apps
  - Haversine (Distance between two GPS coords)
  - Timewrap (Enhanced Time overlay)
  - Levenshtein (Fuzzy string compare)
  - Base64 (Encode/Decode)

For More Information

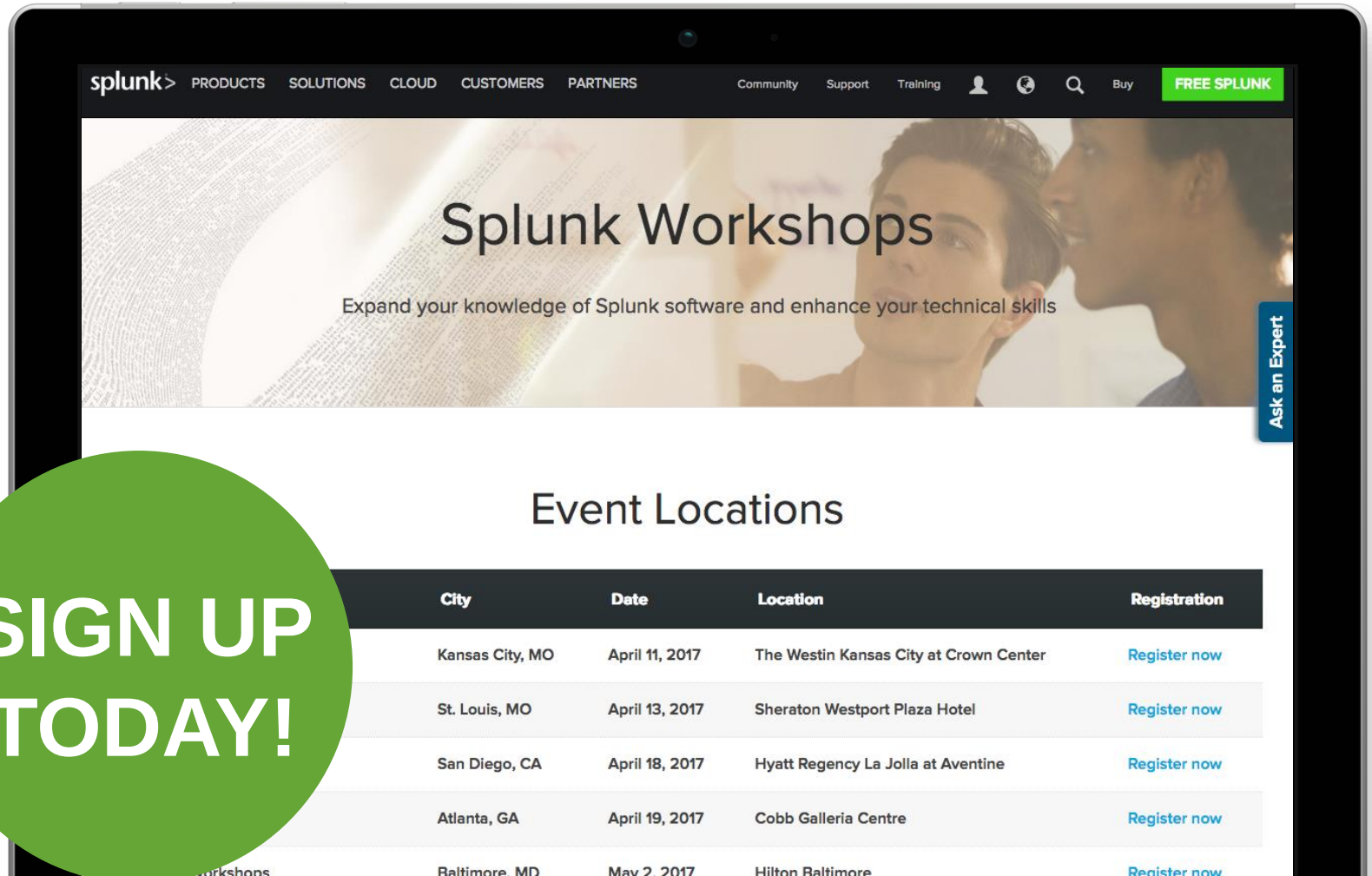
- Additional information can be found in:
  - Power of SPL App!
  - Search Manual
  - Blogs
  - Answers
  - Exploring Splunk

splunk>live!

Workshops: Get Splunk Hands-on Experience

Attend a Splunk Workshop

splunk.com/workshops



SIGN UP TODAY!

May 23: San Francisco

- **Venue:** Sheraton Fisherman's Wharf
- **Time:** 8:30am
- Register Soon!
  - splunk.com/workshops

May 25: Sacramento

- **Venue:** Hyatt Regency Sacramento
- **Time:** 8:30am
- Register Now!
  - splunk.com/workshops

splunk>live!

.conf2017

The 8th Annual Splunk Conference

SEPT 25-28, 2017

Walter E. Washington Convention Center

Washington, D.C.

SAVE OVER $450

You will receive an email after registration opens with a link to save over $450 on the full conference rate.
You'll have 30 days to take advantage of this special promotional rate!

conf.splunk.com

splunk>live!

Take the Survey on Pony Poll

ponypoll.com/slsf

Complete the survey for your chance to win a .conf2017 pass

Q & A

splunk>live!