splunk> .conf2017

Creating Your Own Splunk Learning Environment

Luke Netto | Senior Professional Services Consultant @ Splunk

September 26, 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

Who Are You?

- You have Splunk installed
- You know how to create dashboards
- You want to increase your knowledge of SPL
- You want to teach coworkers SPL outside of production
- Hopefully, you brought your laptop

Who Am I?

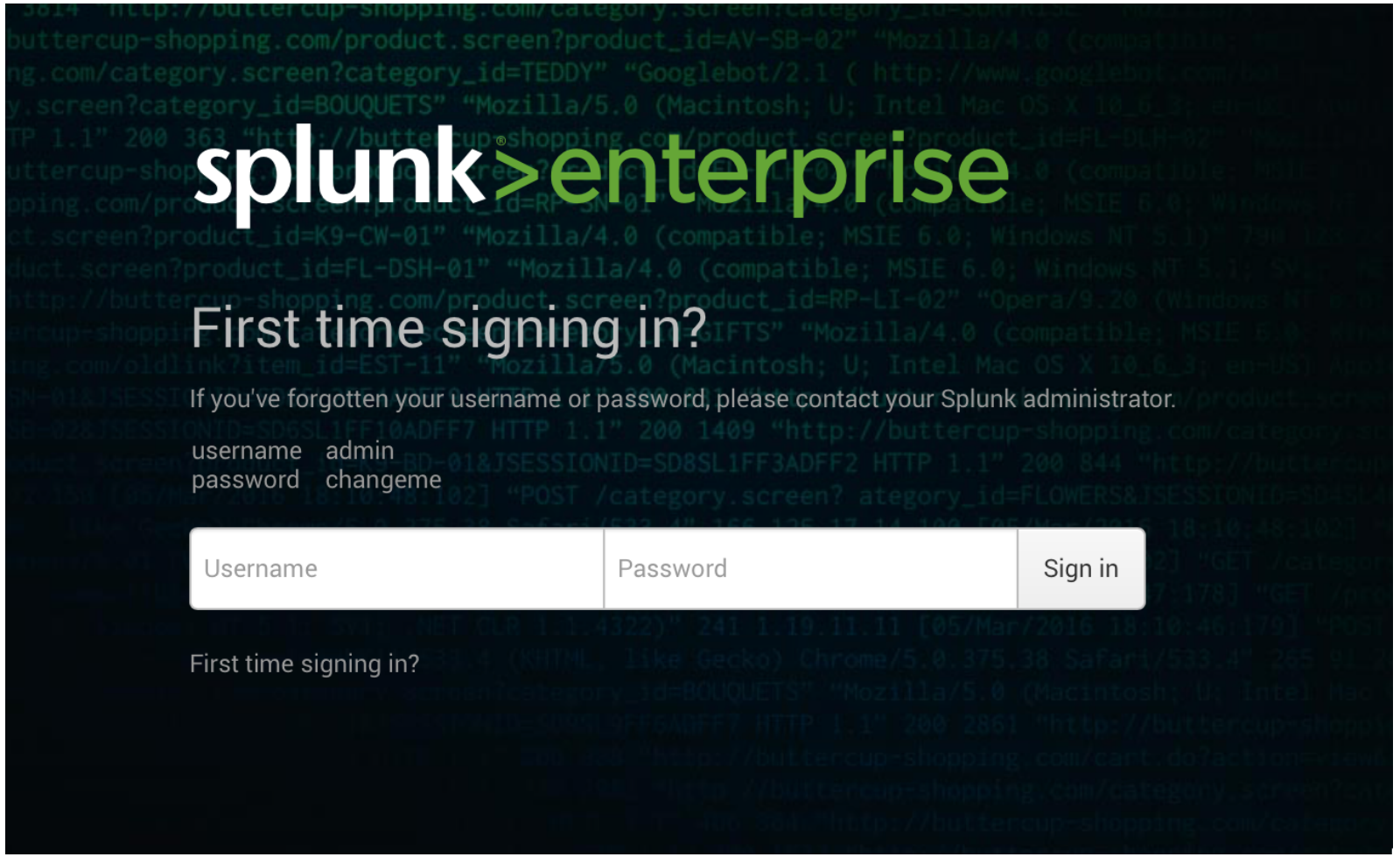
- 3+ years of Splunk experience
- 7+ years of systems engineering
- 5+ years of data analytics
- systems engineering + data analytics = Splunk

Download & Install Splunk

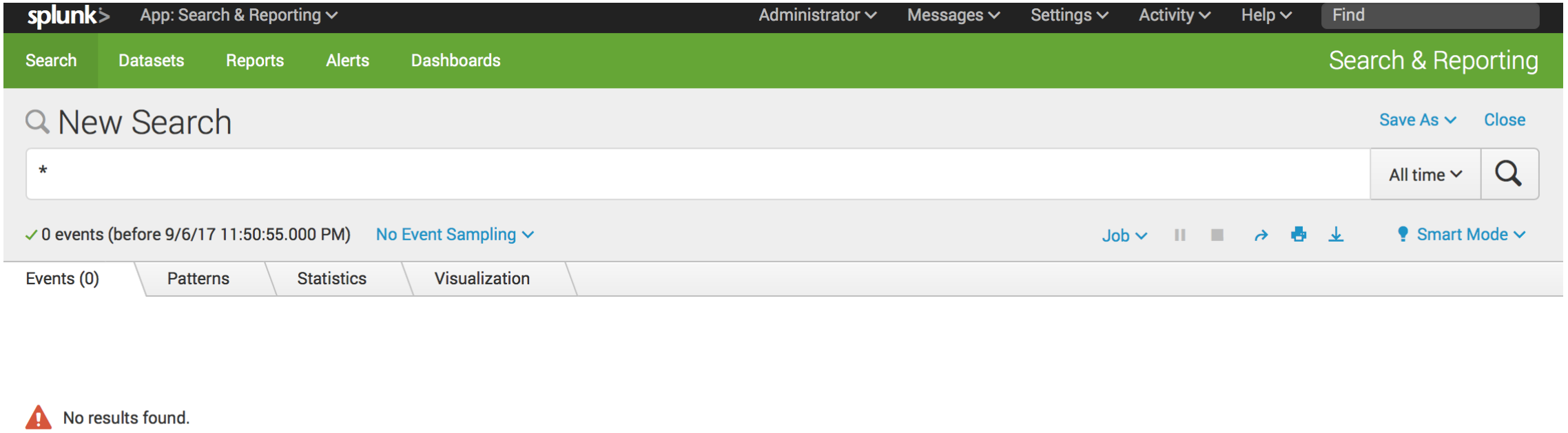
splunk> .conf2017

Login

localhost:8000

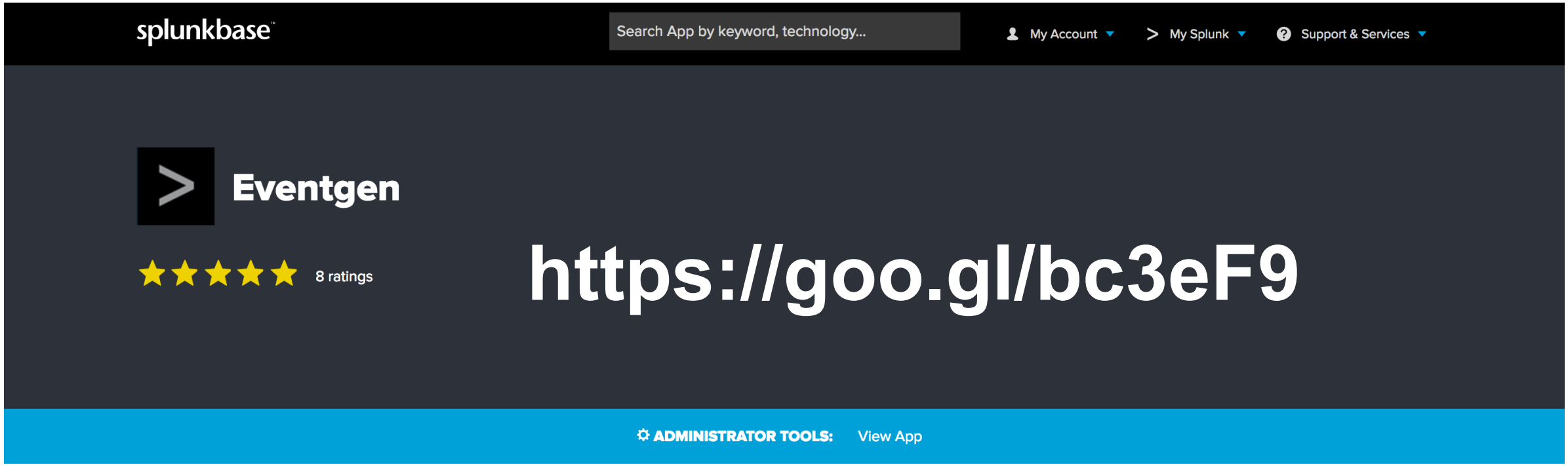


No Data ☹



Download Eventgen

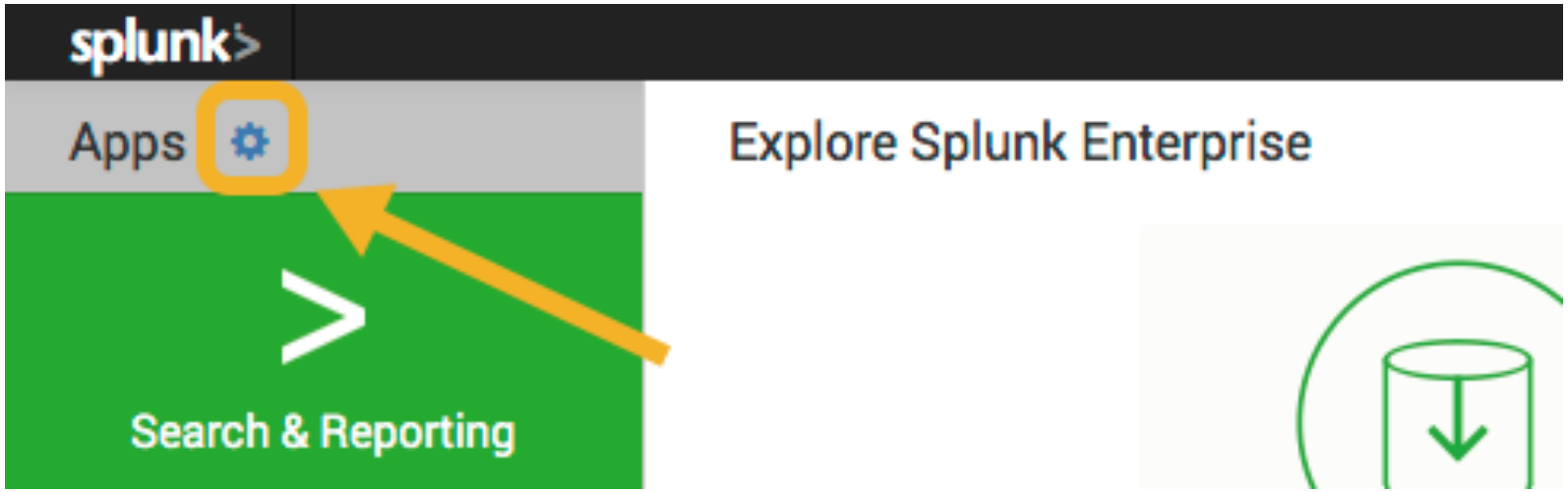
https://splunkbase.splunk.com/app/1924/



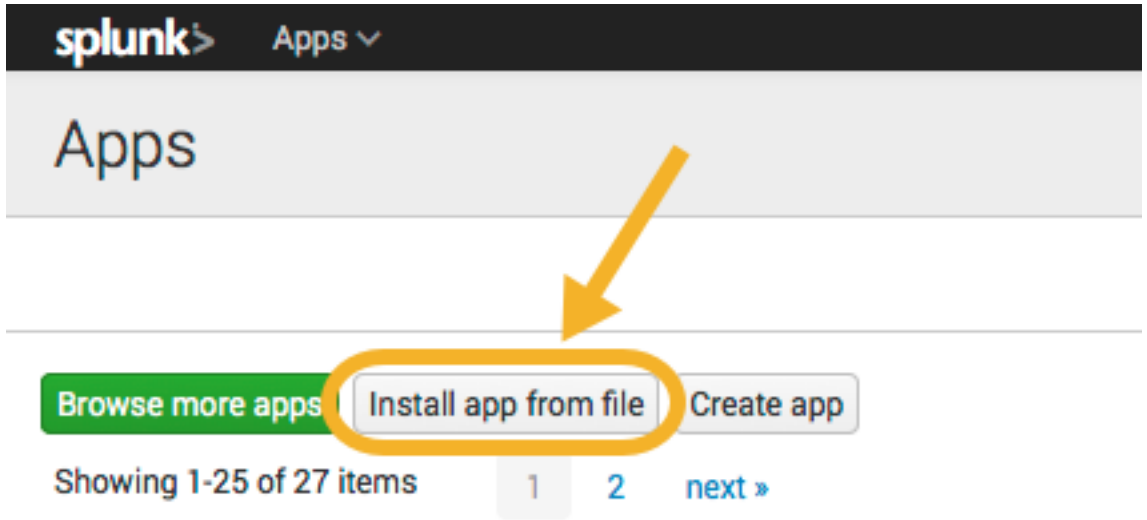
splunk> .conf2017

Install The App

From the Splunk Web home screen, click the gear icon next to **Apps**.

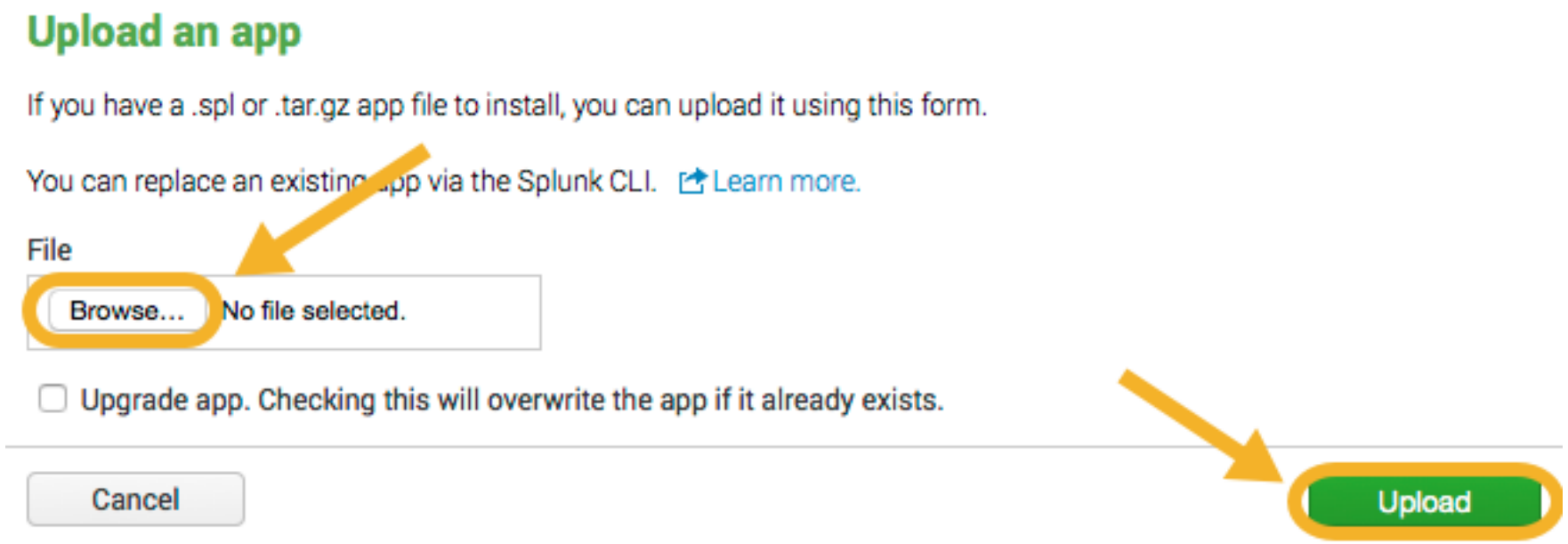


Click Install App From file

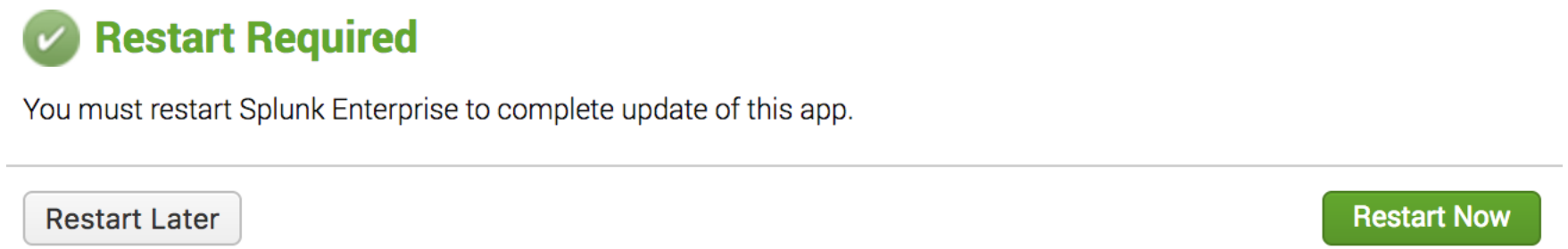


Upload An App

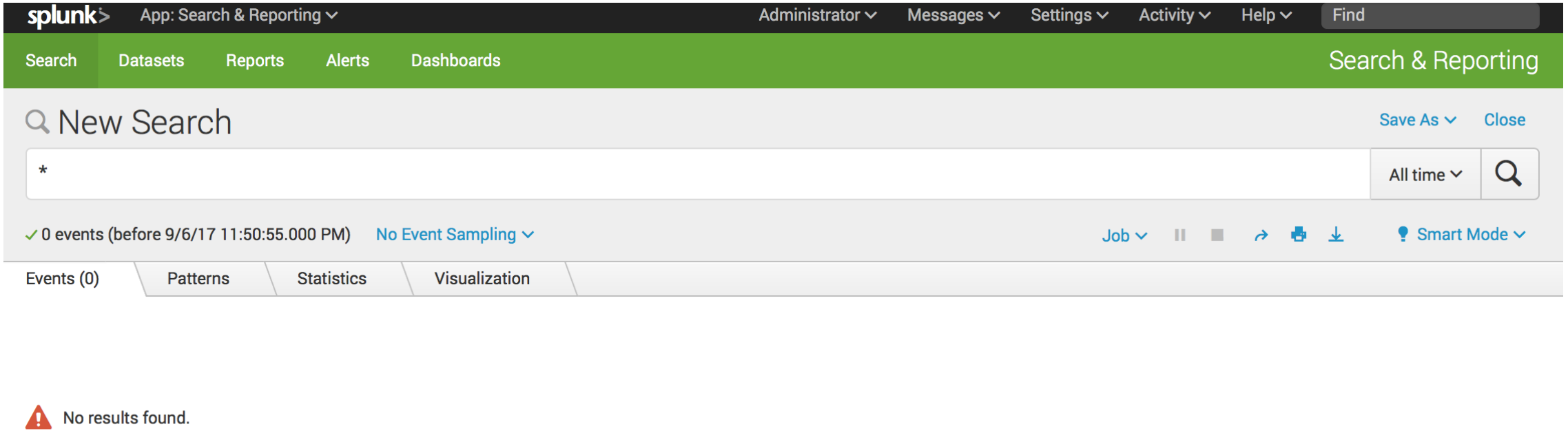
Locate the downloaded file and click **Upload** (SA-Eventgen.spl)



Restart Splunk

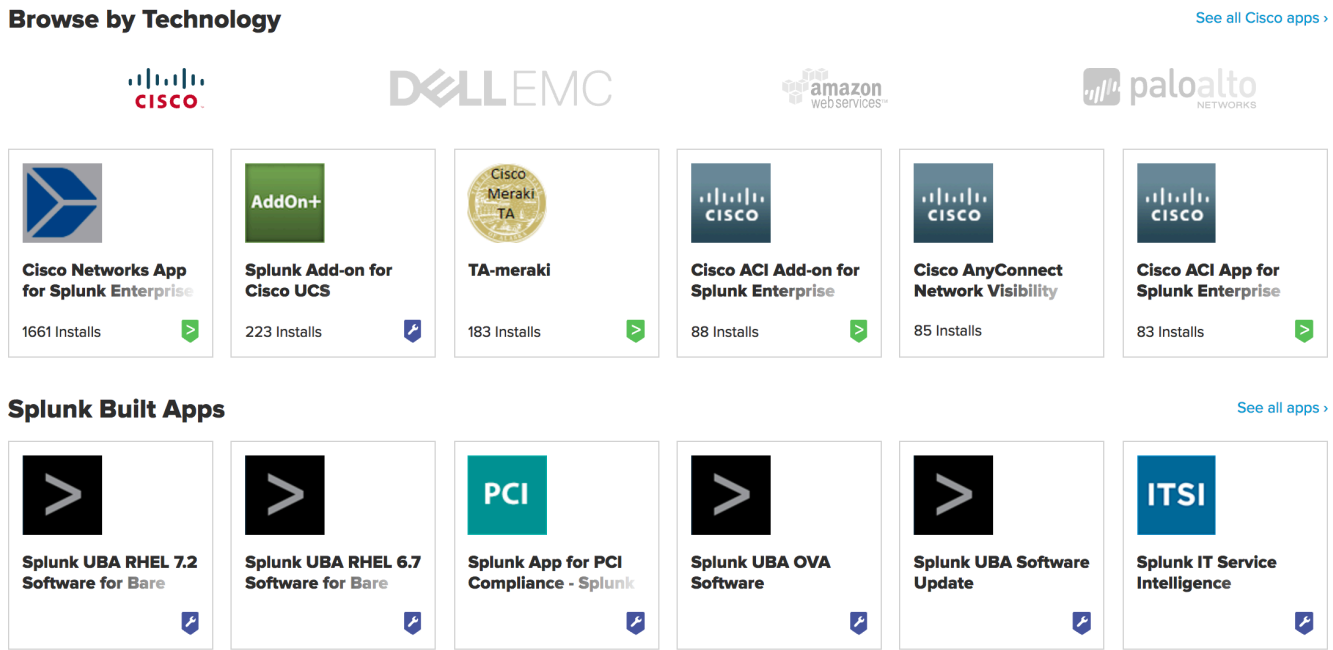


Still No Data ☹



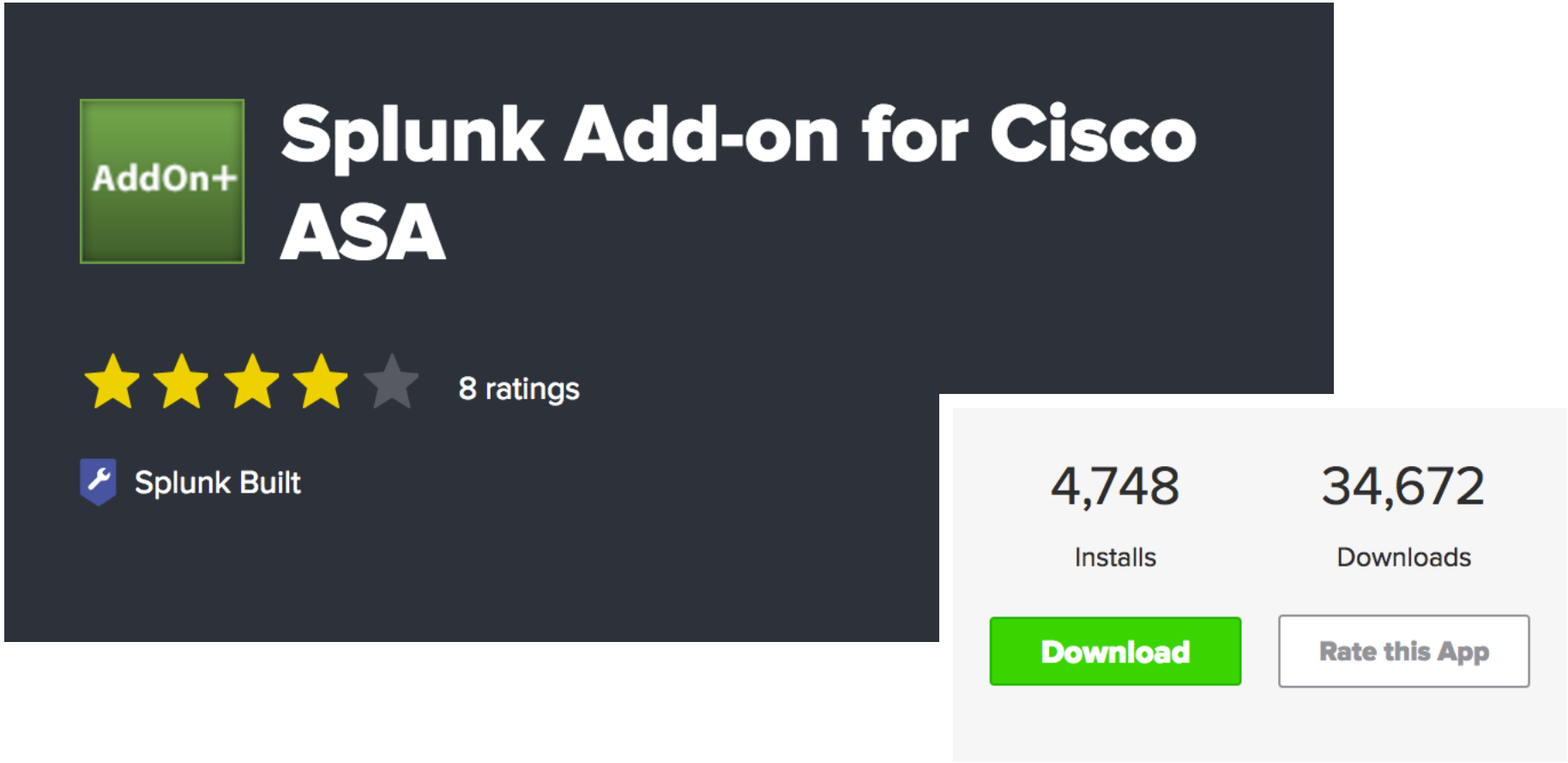
Let's Grab an App

Where do you get Apps? Splunkbase!



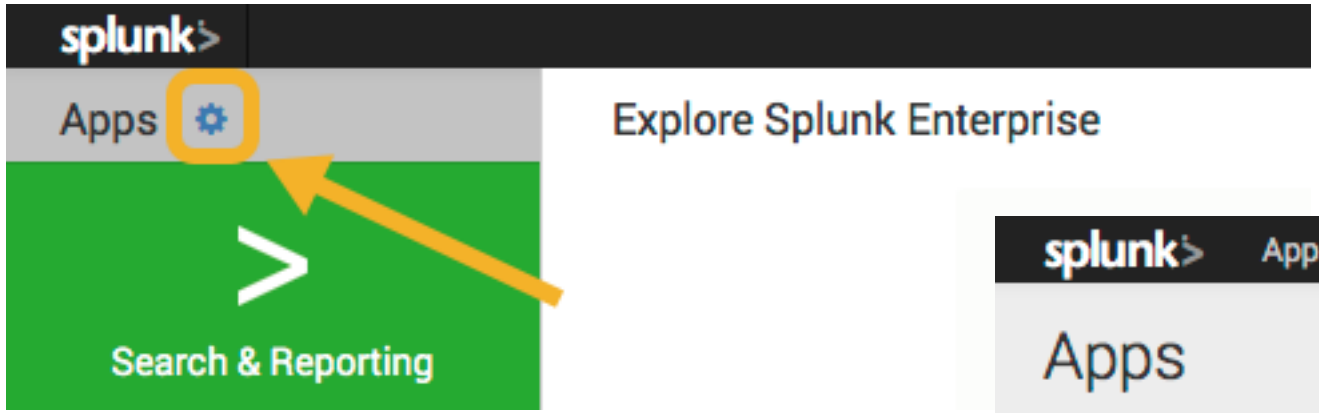
How About This One?

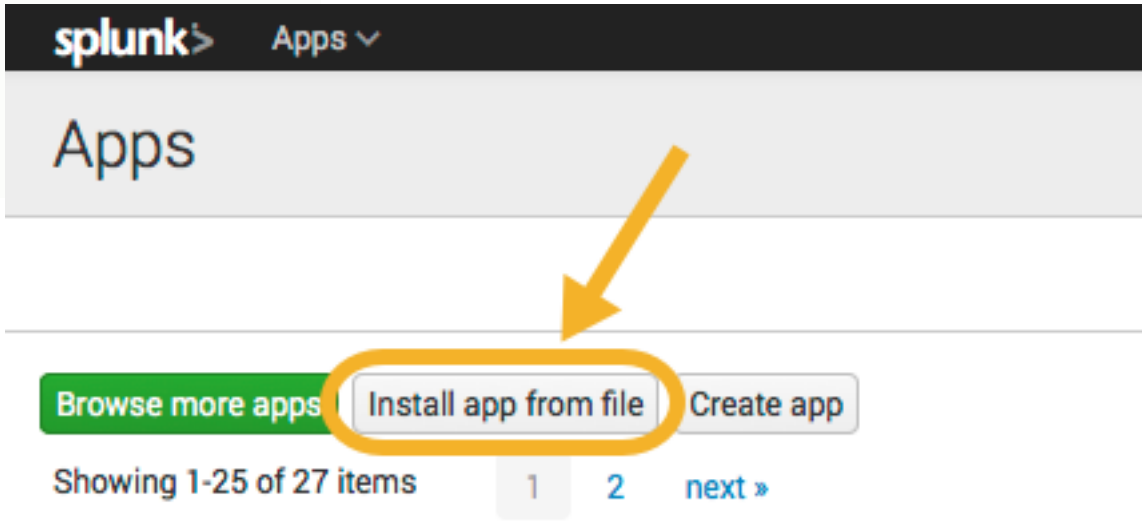
https://splunkbase.splunk.com/app/1620/



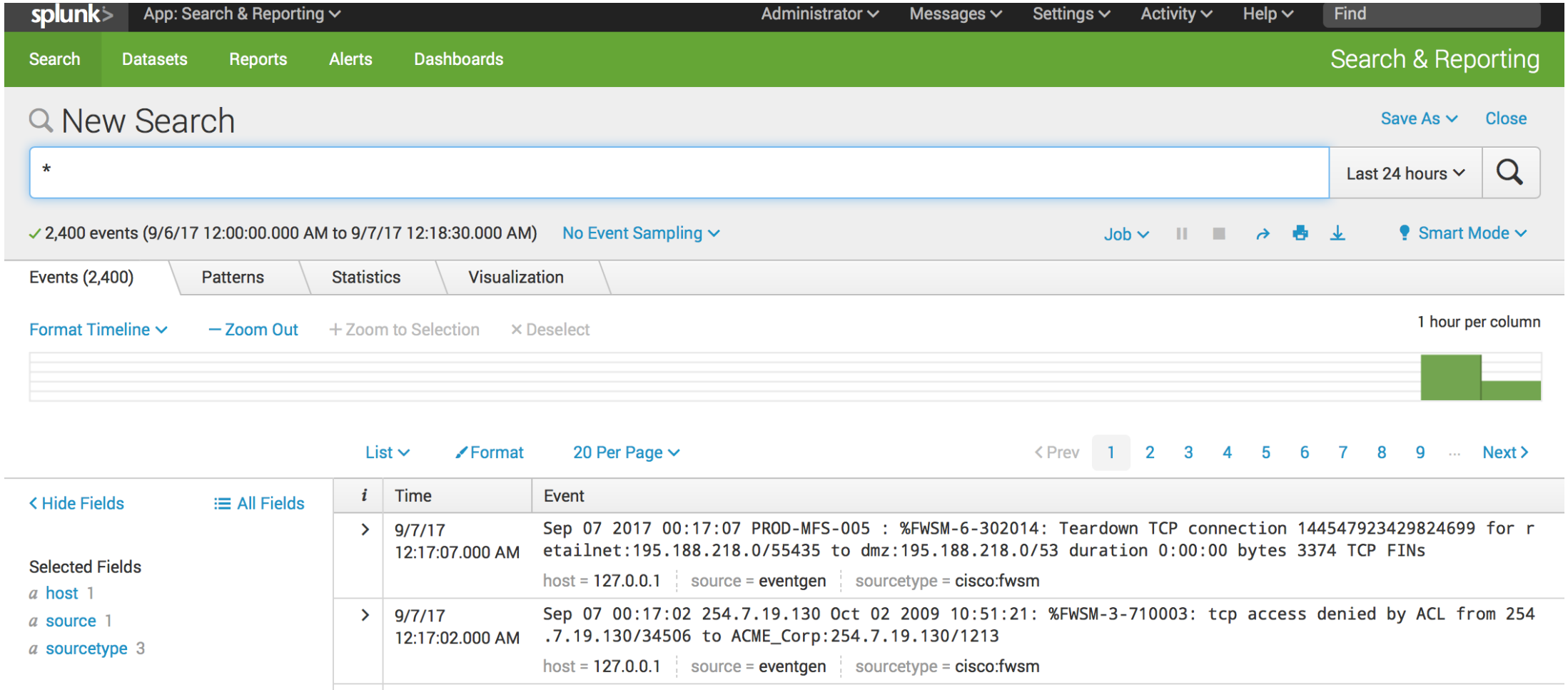
Install The App

Rinse and Repeat





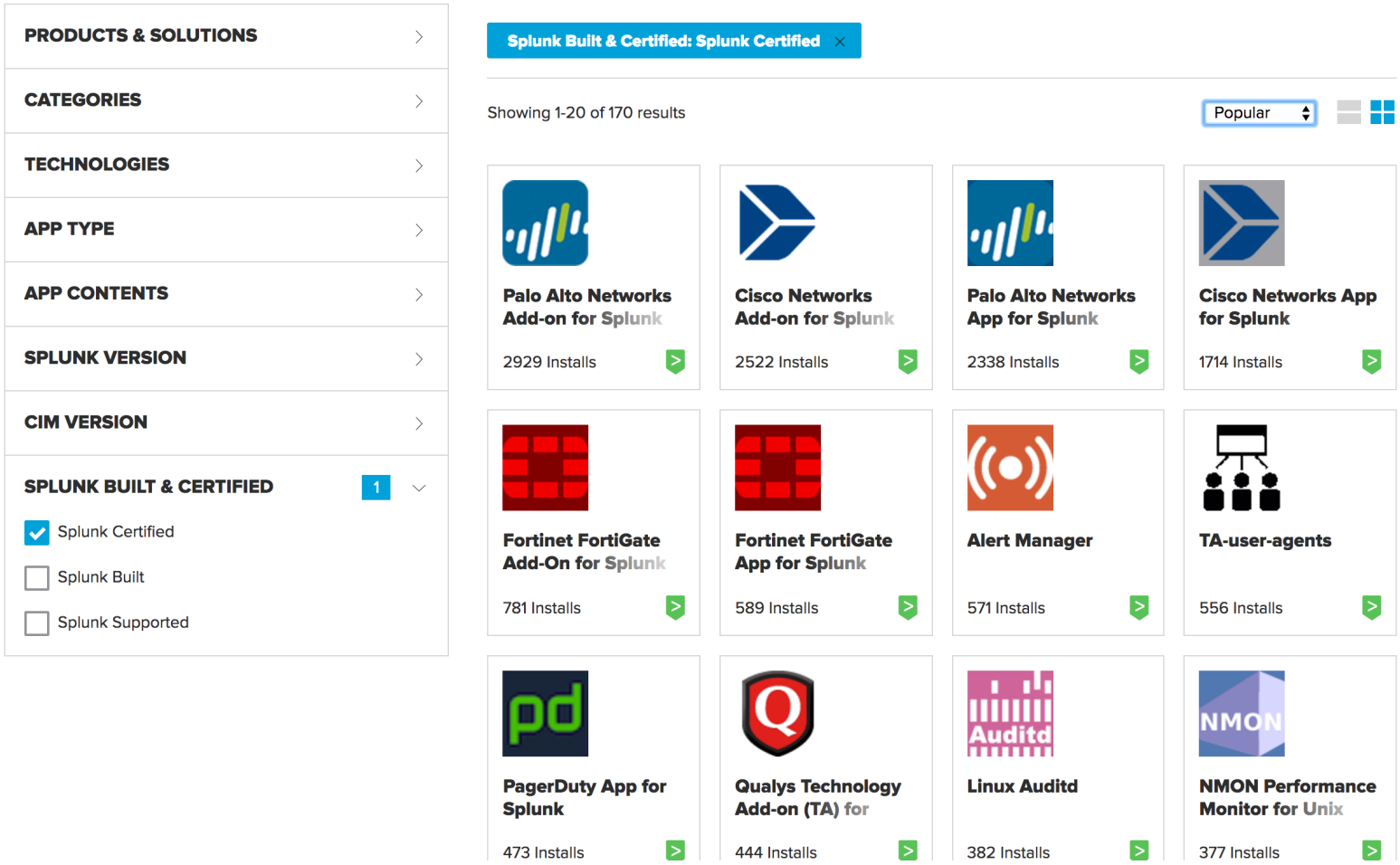
We Have Data ☺



splunk> .conf2017

What Apps Work?

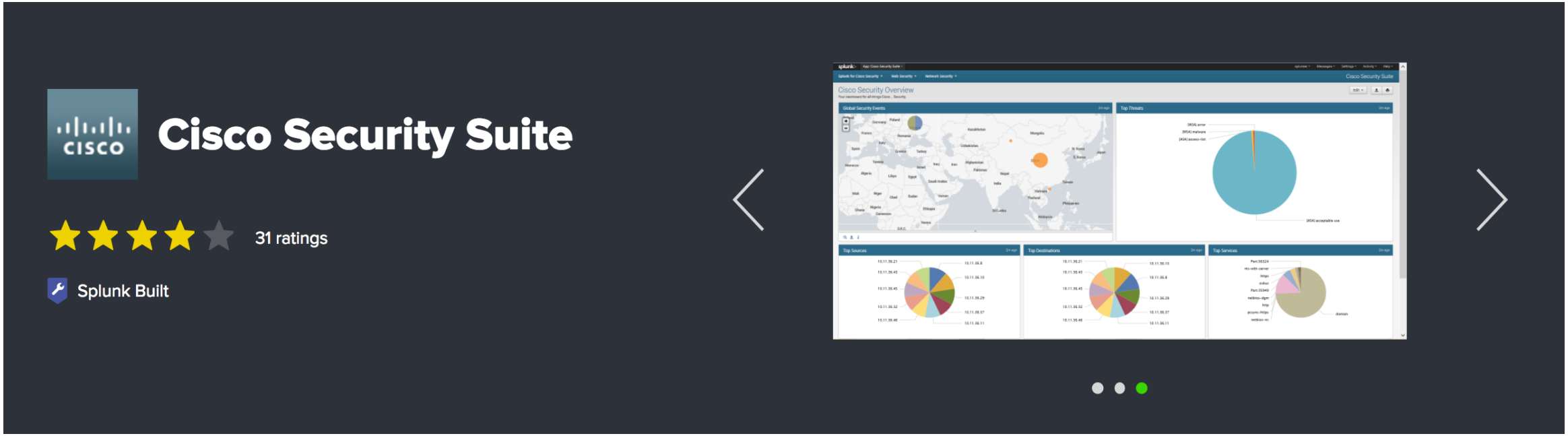
Anything that is Splunk certified and/or has an eventgen.conf file!



splunk> .conf2017

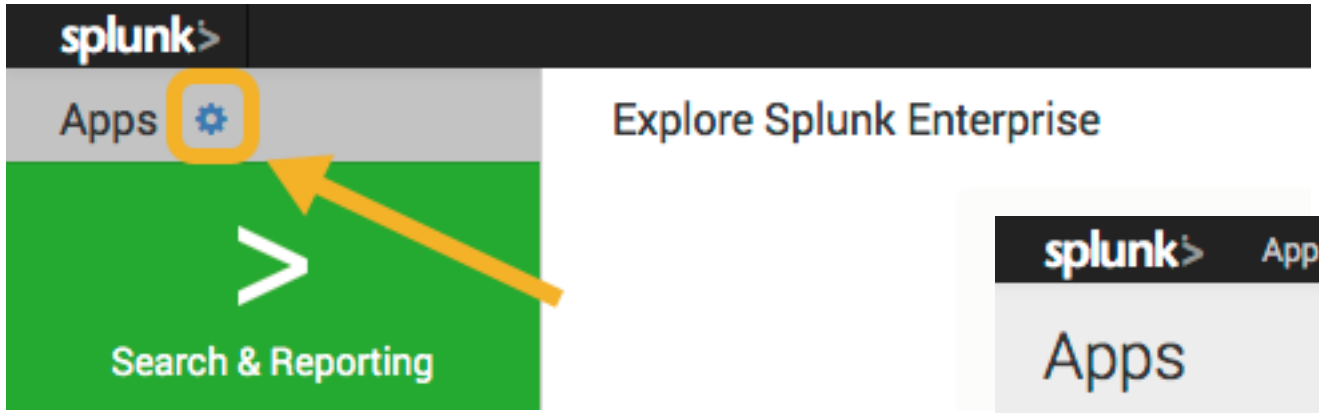
What Else Can You Do?

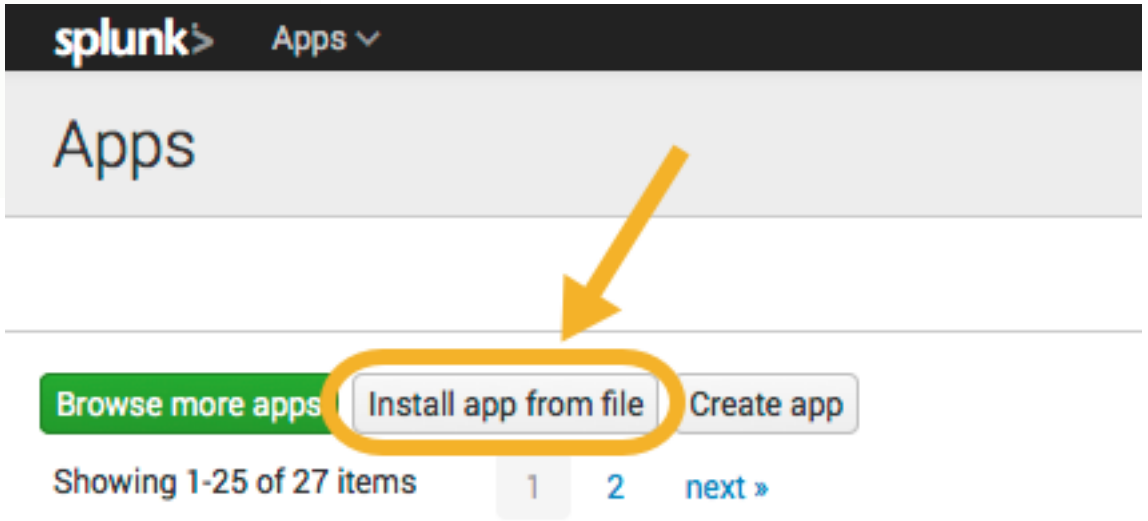
https://splunkbase.splunk.com/app/525/



Install The App

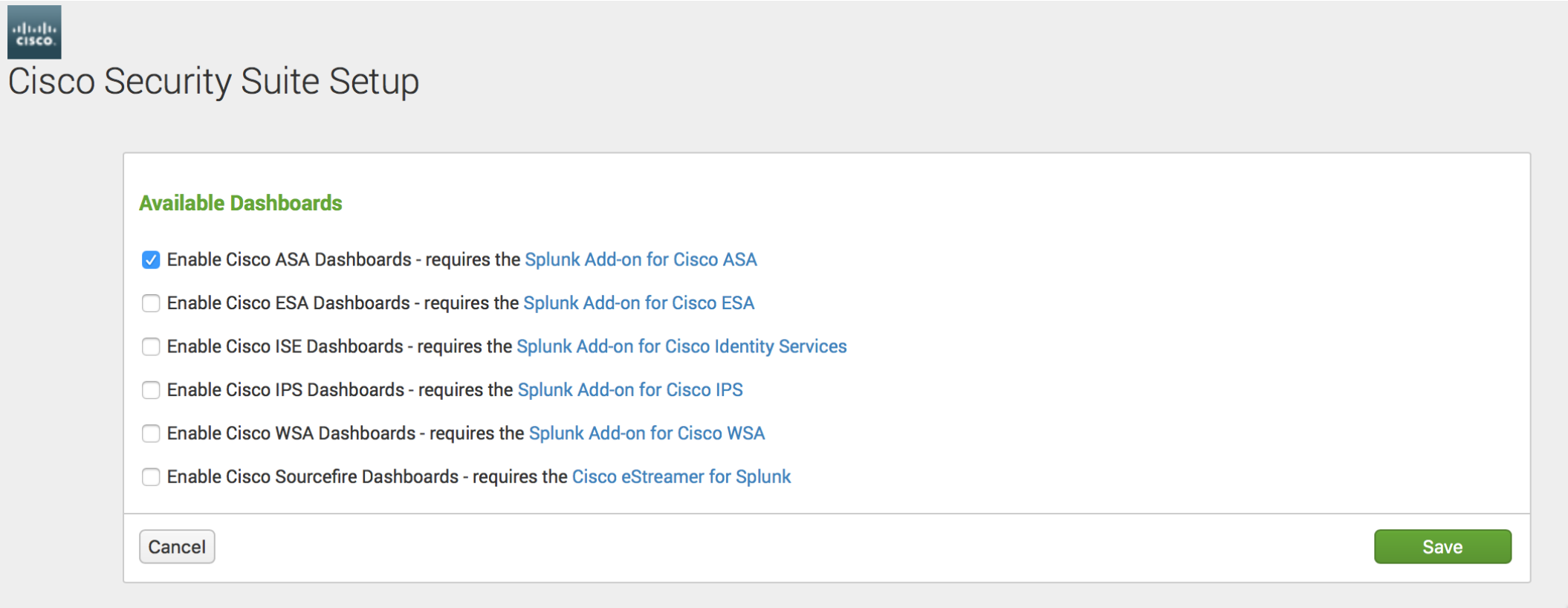
Rinse and Repeat



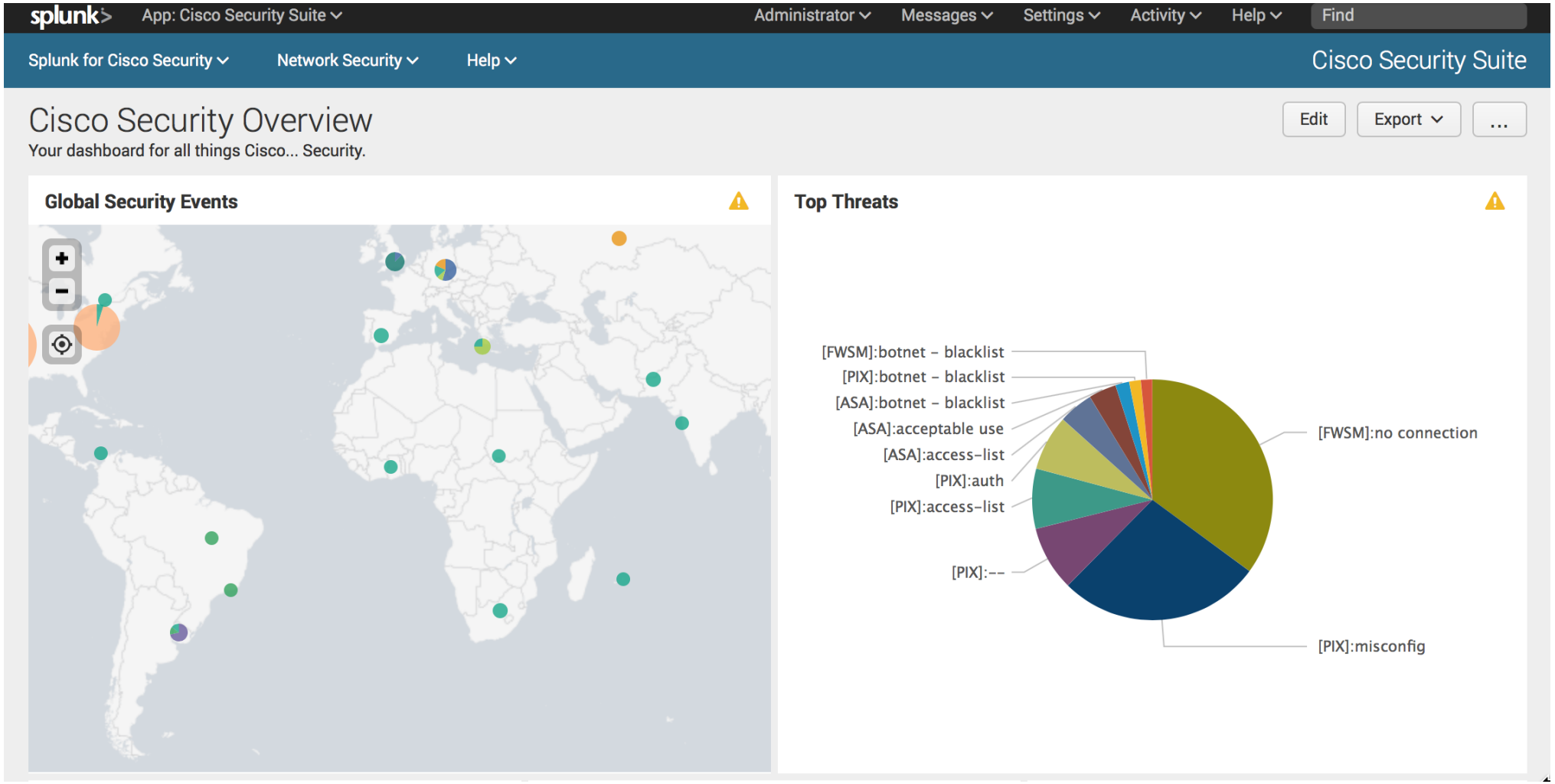


Setup

Since we've only installed the Add-on for Cisco ASA

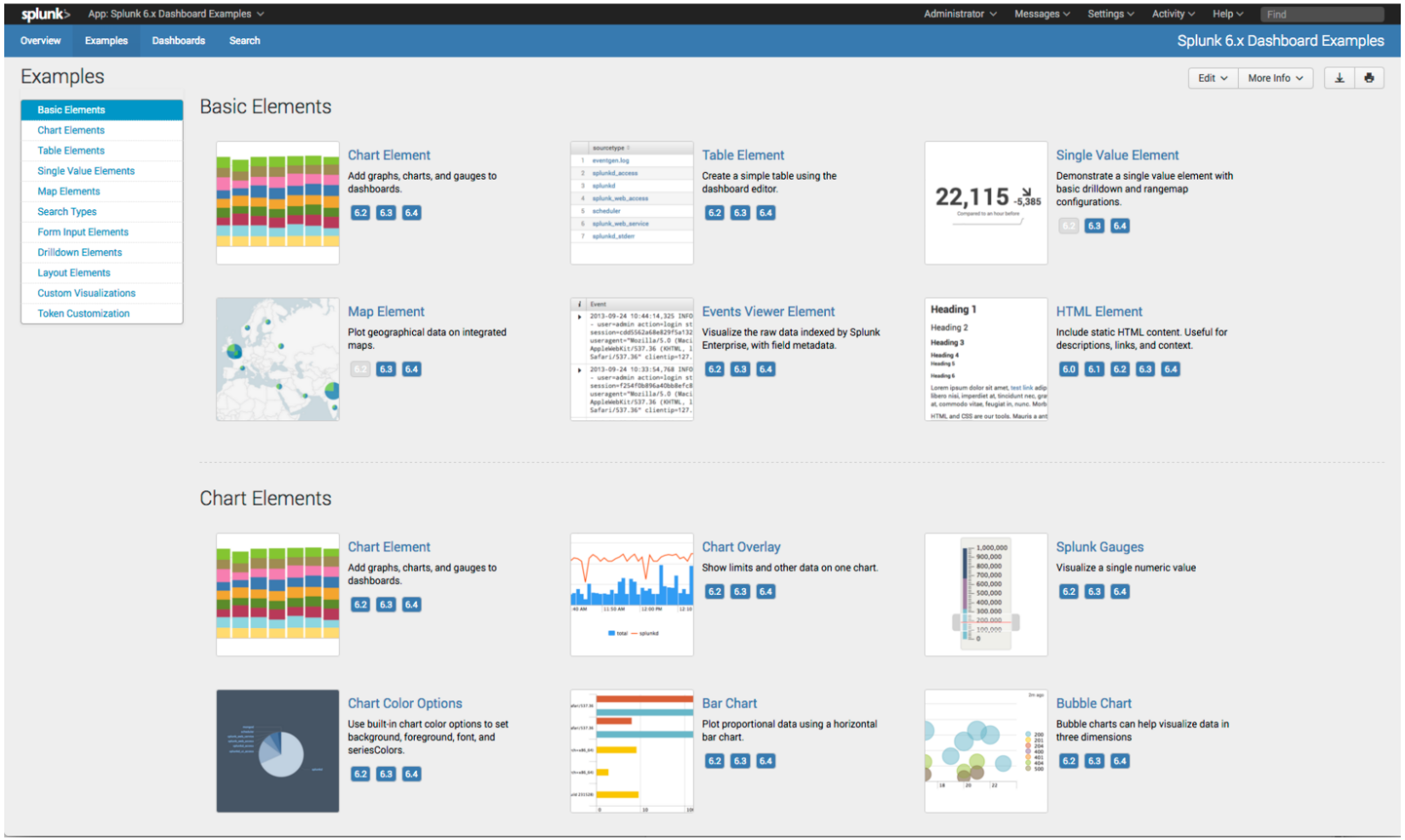


Dashboards!



Splunk 6.x Dashboard Examples

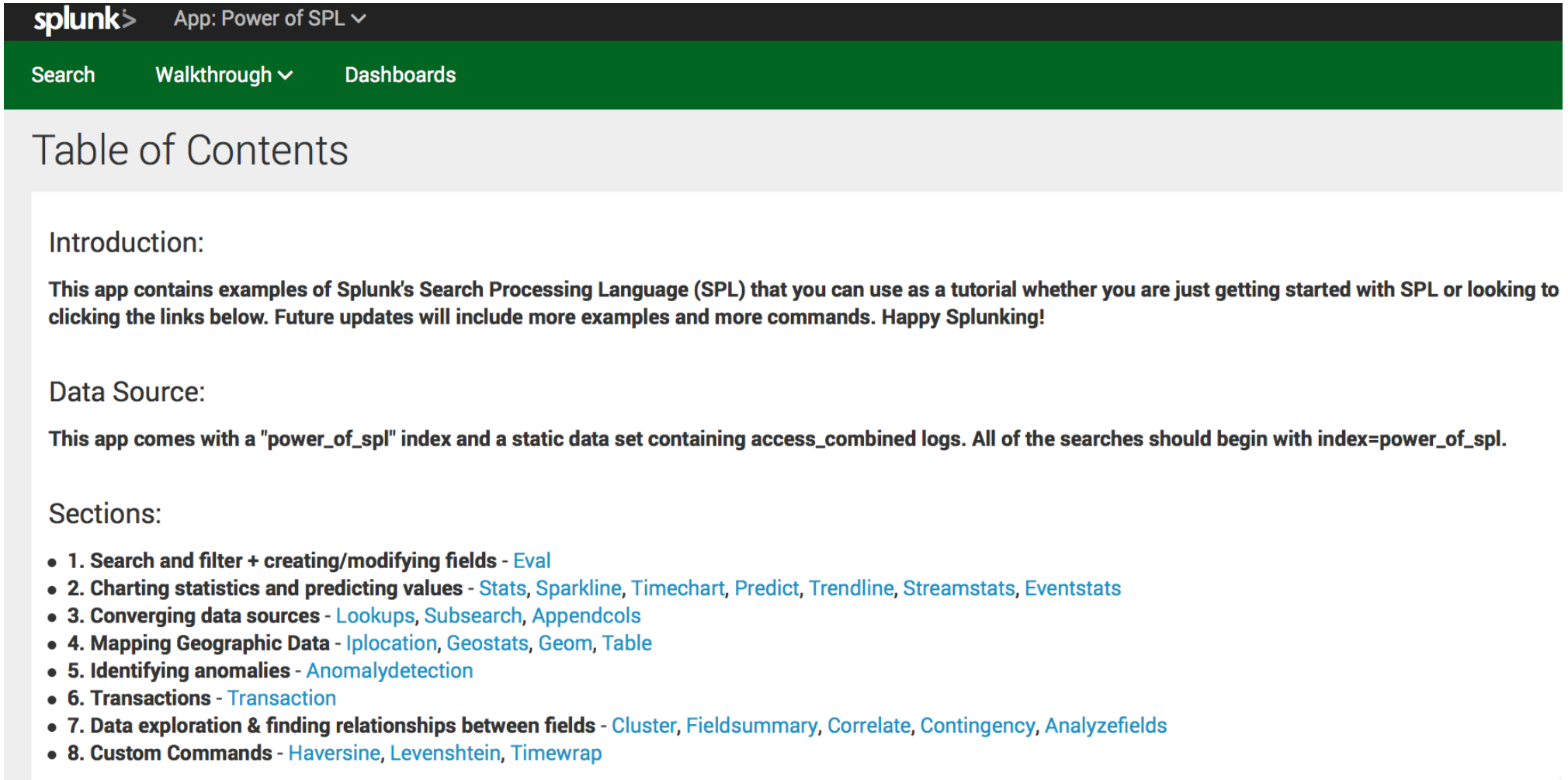
https://splunkbase.splunk.com/app/1603/



splunk> .conf2017

Power of SPL

https://splunkbase.splunk.com/app/3353/



splunk> .conf2017

Stats Examples

2.1 Stats Examples

Edit | Export | ...

Pick a Stats Example:

Basic Stats & Rename
Multiple Statistics
Stats By Another Field

Hide Filters

Basic Stats & Rename

index=power_of_spl
| **stats** avg(bytes) **AS** "Avg Bytes"

Avg Bytes
4973.068211993804

Multiple Statistics

index=power_of_spl
| stats **avg**(bytes) AS bytes **sparkline**(avg(bytes)) AS Bytes_Trend **min**(bytes) as Min **max**(bytes) as Max

bytes	Bytes_Trend	Min	Max
4973.068211993804		100	59994

Stats By Another Field

index=power_of_spl
| stats avg(bytes) AS avg_bytes sparkline(avg(bytes)) AS Bytes_Trend min(bytes) as Min max(bytes) as Max **by** clientip | sort - avg_bytes

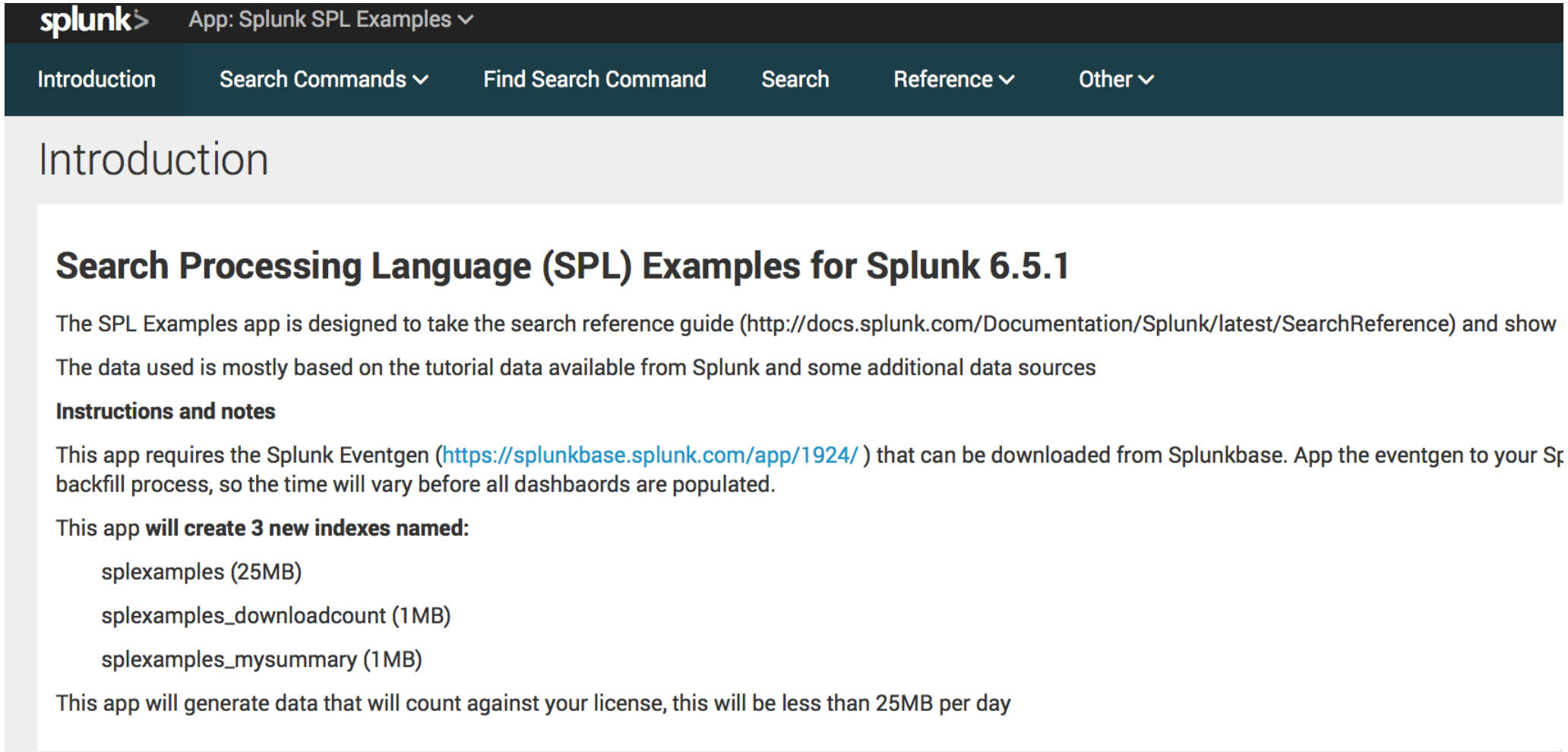
clientip	avg_bytes	Bytes_Trend	Min	Max
175.45.177.7	46638.01379310345		30198	59951
175.45.177.11	46343.56934306569		30539	59994
175.45.177.17	46043.95333333333		30143	59859
183.97.189.111	45766.18831168831		31479	59983
175.45.177.189	45471.924812030076		30430	59917

« prev 1 2 3 4 5 6 7 8 9 10 next »

splunk> .conf2017

Splunk SPL Examples

https://splunkbase.splunk.com/app/3456/



splunk> .conf2017

Let's Learn "predict"

Introduction | Search Commands | Find Search Command | Search | Reference | Other | Splunk SPL Examples

predict

Edit | Export | ...

Description

The `predict` command forecasts values for one or more sets of time-series data. The command can also fill in missing data in a time-series and provide predictions for the next several time steps.

The `predict` command provides confidence intervals for all of its estimates. The command adds a predicted value and an upper and lower 95th percentile range to each event in the time-series. See the **Usage** section in this topic.

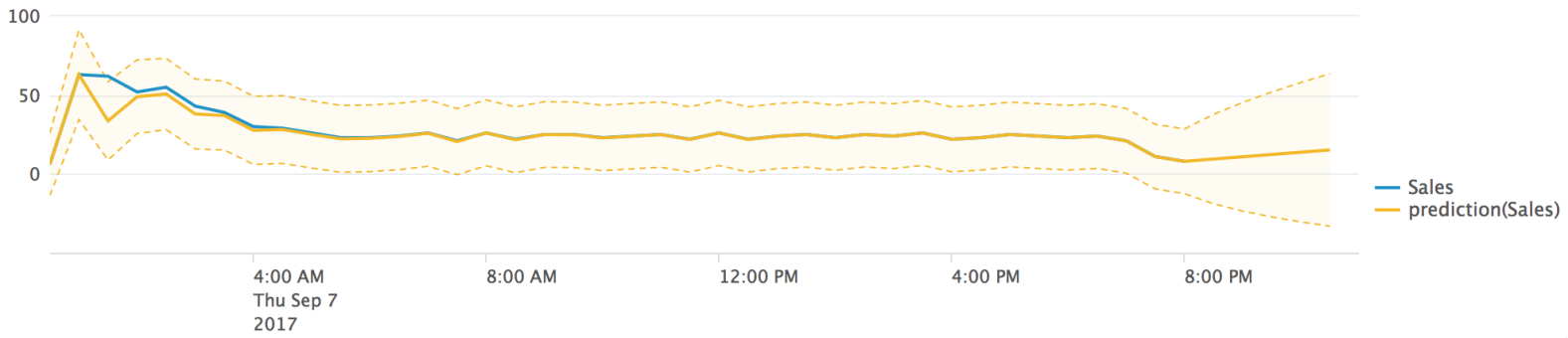
Syntax

predict <field-list> [AS <newfield>] [<predict_options>]

Example 1

Predict future sales based on the previous sales numbers.

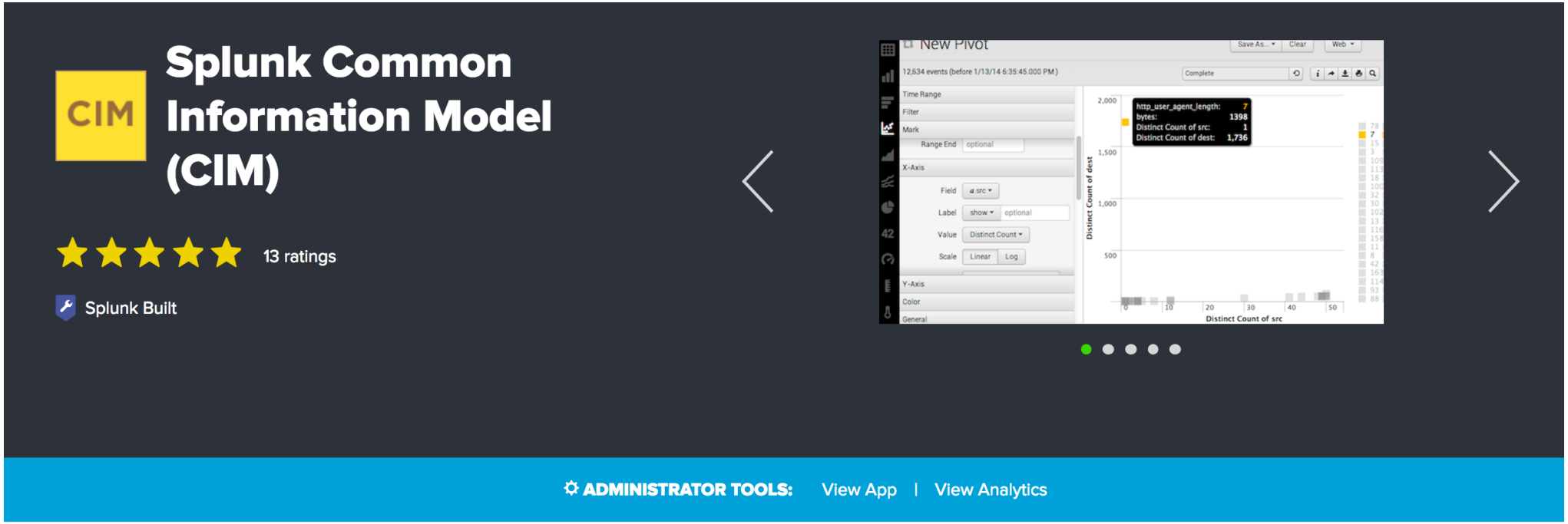
Search: index=splexamples sourcetype=vendor_sales | timechart count as Sales | predict Sales



splunk> .conf2017

Going Beyond

https://splunkbase.splunk.com/app/1621/



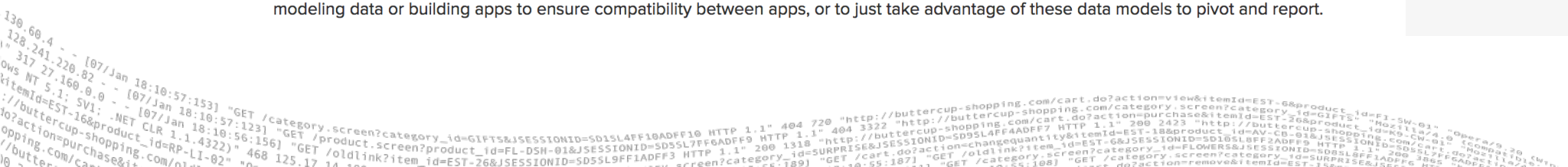
Overview | Details

The Common Information Model is a set of field names and tags which are expected to define the least common denominator of a domain of interest. It is implemented as documentation on the Splunk docs website and JSON data model files in this add-on. Use the CIM add-on when modeling data or building apps to ensure compatibility between apps, or to just take advantage of these data models to pivot and report.

5,393 Installs

28,683 Downloads

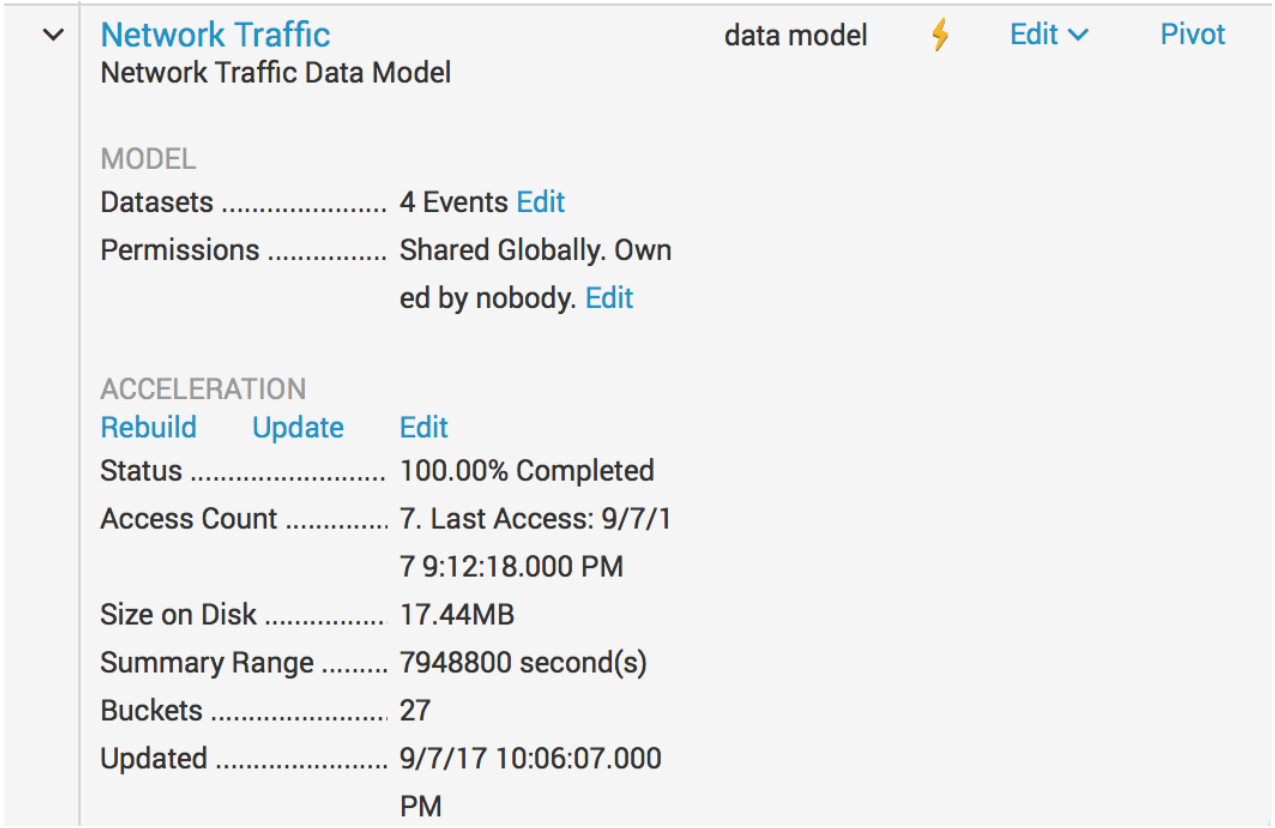
Download | Rate this App



splunk> .conf2017

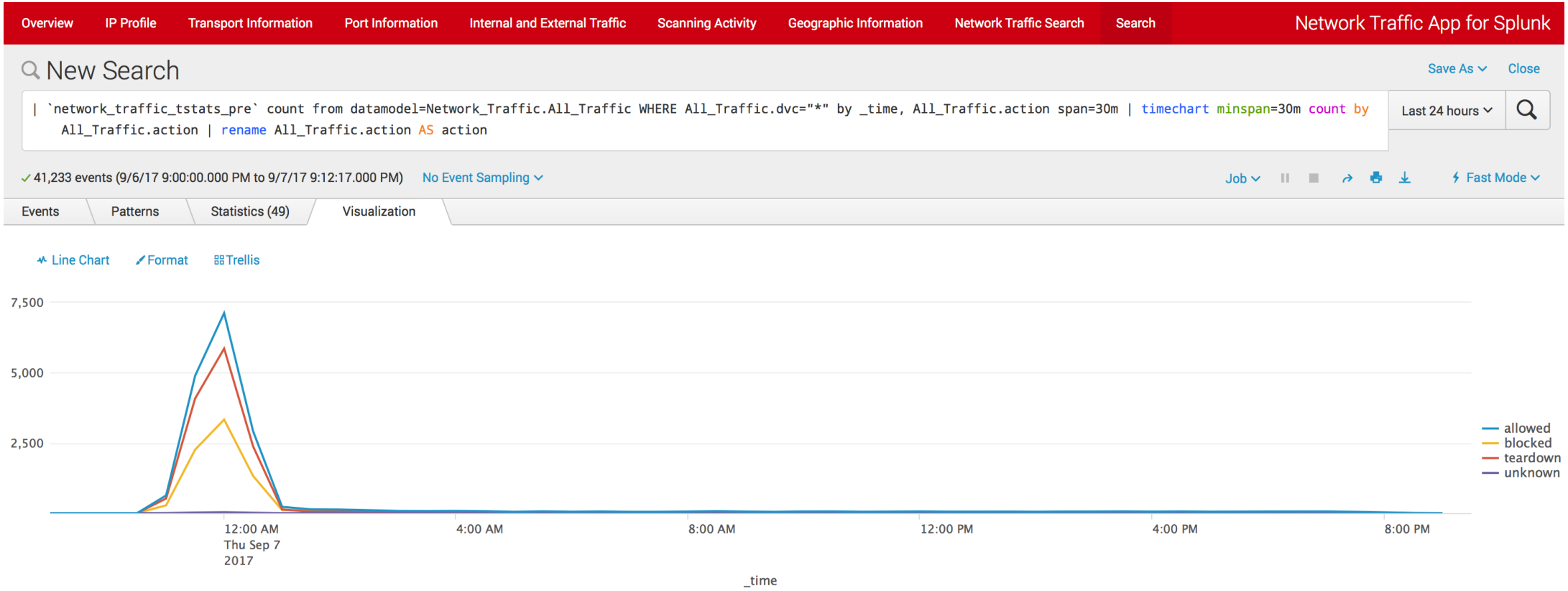
Learn Data Models

- After installing the CIM app, enable data model acceleration where appropriate and practice tstats and datamodel searches



Network Traffic App for Splunk

https://splunkbase.splunk.com/app/3327



splunk> .conf2017

Keep Your Environment Running

Request a Test/Dev license

https://www.splunk.com/en_us/resources/personalized-dev-test-licenses.html

splunk> .conf2017

Even More Data

- Check out gogen, made by the same author as eventgen
  - https://github.com/coccyx/gogen
- Fake-factory, a Python library
  - https://www.blog.pythonlibrary.org/2014/06/18/python-create-fake-data-with-faker/
- Splunk Data Simulator

What's Next?

- Splunk Fundamentals 1 (https://splunk.com/view/SP-CAAAPX9)
- Splunk Fundamentals 2 (https://splunk.com/view/SP-CAAAPYB)

- Go see these sessions (or watch them afterwards)….
  - Sandboxing with Splunk (with Docker)
  - Dashboard Wizardry
  - Dashboards, Alerting, Reporting and Visualization - What's New
  - Focus the Splunk Lens With Visual Design Best Practices
  - Next Generation Dashboards

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