

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, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.



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



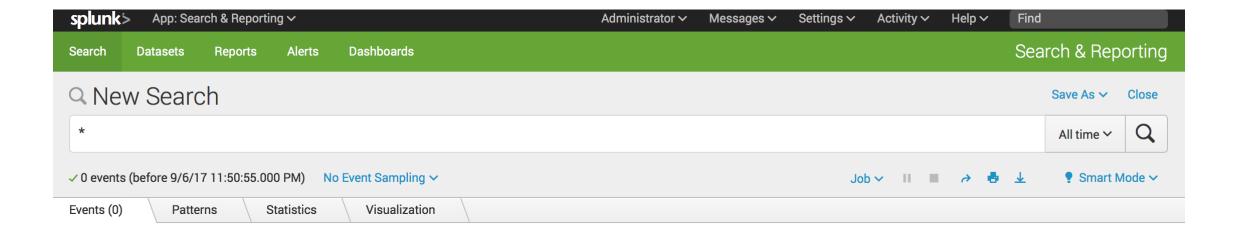


Login localhost:8000

buttercup-shopping.com/product.sc ng.com/category.screen?category_i y.screen?category_id=BOUQUETS" "M TP 1.1" 200 363 "http://butte-tup uttercup-shopSplunkr pping.com/product_id=K9-CW-01" "M	com/category.screen/category.s	"Mozilla/4.0 (compatinis: http://www.googlebot.com/bol Intel Mac OS X 10_6_3; en to e-?product_id=FL-DLH-62* "ISE 0 (compatible MAI (Compatible; MSIE 6.0; Windows IE 6.0; Windows NT 5.1) 790 12	
First time significant of the si	duct. screen?product_id=RP-Igning in? IFTS" "Mozil Mozilla/5.0 (Macintosh; U; rname or password, please contact HTP 1.1" 200 1409 "http:// JSESSIONID=SD8SL1FF3ADFF2 I "POST /category.screen? a	LI-02" "Opera/9.20 (Windows III lla/4.0 (compatible; MSIE E Intel Mac OS X 10.6.39 en-US) t your Splunk administrator. /buttercup-shopping.com/category HTTP 1.1" 200 844 "http://www.tegory_id=FLOWERS&JSESSION.D=S0-	
Username	Password	Sign in	
First time signing in?			



No Data ⊗

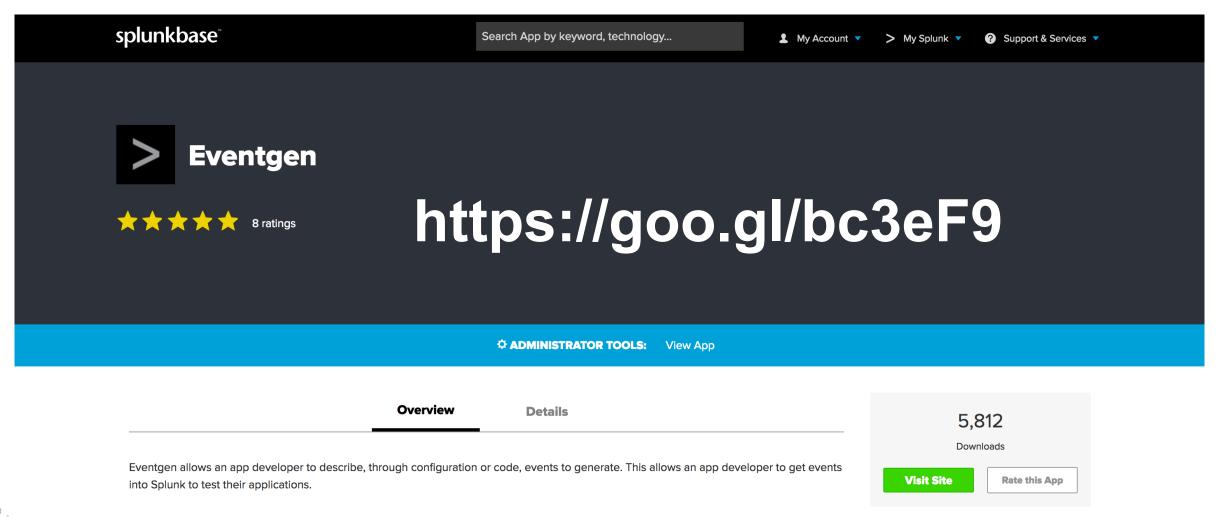


A No results found.



Download Eventgen

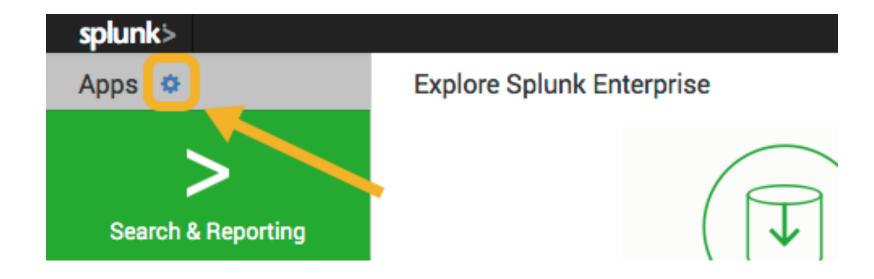
https://splunkbase.splunk.com/app/1924/





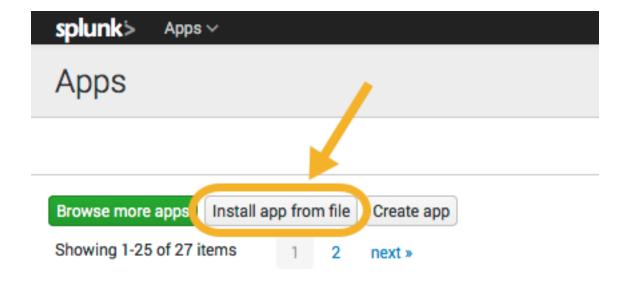
Install The App

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





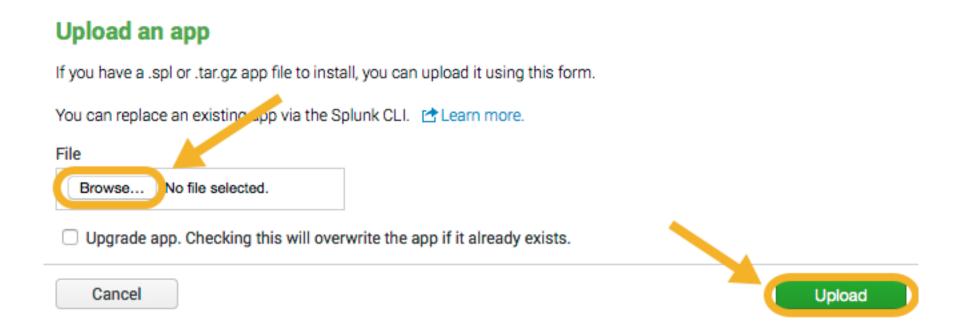
Click Install App From file





Upload An App

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





Restart Splunk



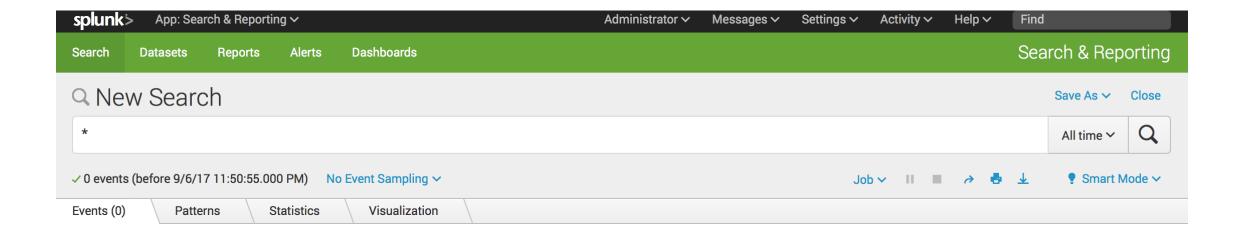
You must restart Splunk Enterprise to complete update of this app.

Restart Later

Restart Now



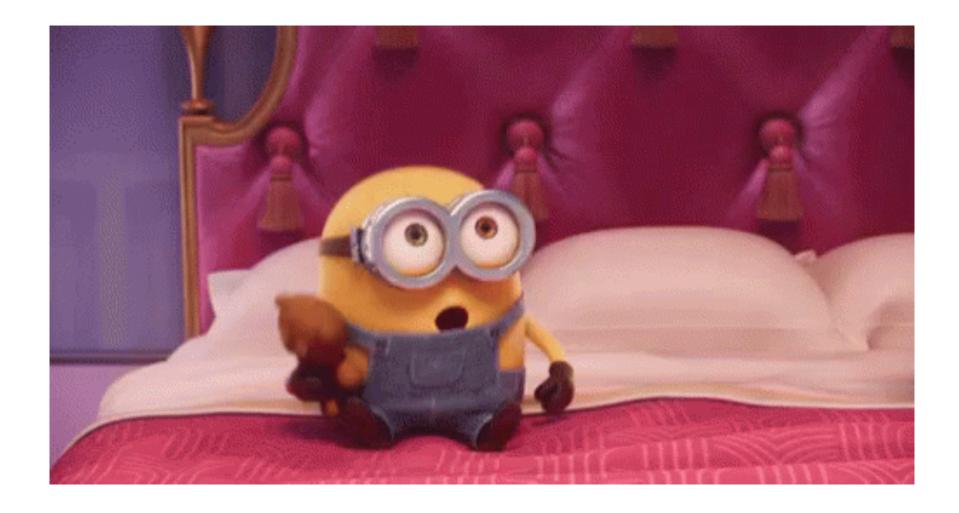
Still No Data ⊗



A No results found.



Let's Grab an App



"GET /product.screen?roduct_id=FL-DSH-D1&JSESSIONID=SD1SL4FF10ADFF10 HTTP 1.1" 404 729 "http://buttercup-shoppinto-"GET /product.screen?roduct_id=FL-DSH-D1&JSESSIONID=SD3SL7FF0ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shoppinto-125.17 14 cold link?id=ET-JSEN-SESSIONID=SD3SL7FF0ADFF0 HTTP 1.1" 200 1318 "http://buttsfionid=SD3SL4FFADFF0 125.17 14 cold link?id=ET-JSEN-SESSIONID=SD3SSL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttsfionid=SD3SL3FFADFF0 HTT



Where do you get Apps? Splunkbase!



Browse by Technology





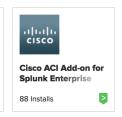
















See all apps >

See all Cisco apps >

Splunk Built Apps



do:10:57:153] "GET /Category.screen?category_id=GIFTS&15E5510NID=SD15L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping-local lib:10:57:123] "GET /Category.screen?category_id=GIFTS&15E5510NID=SD15L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping-category_id=GIFTS&15E5510NID=SD15L4FF10ADFF10 HTTP 1.1"







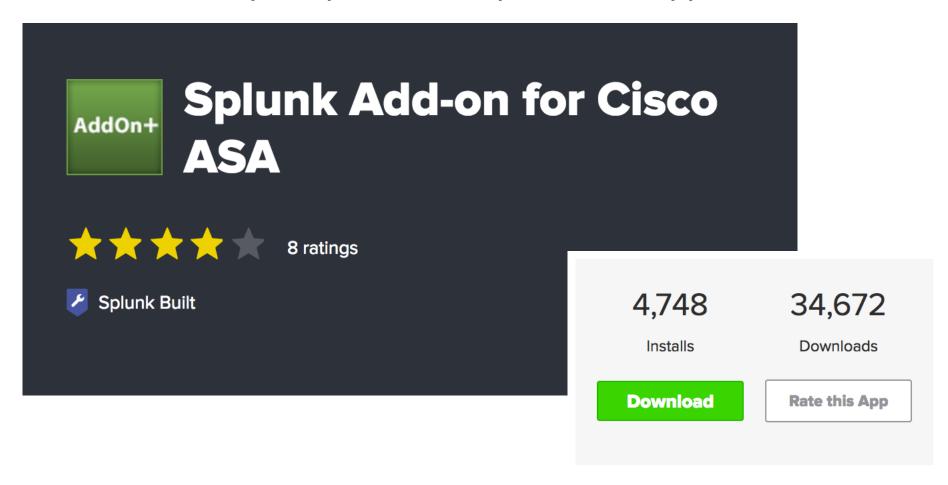






How About This One?

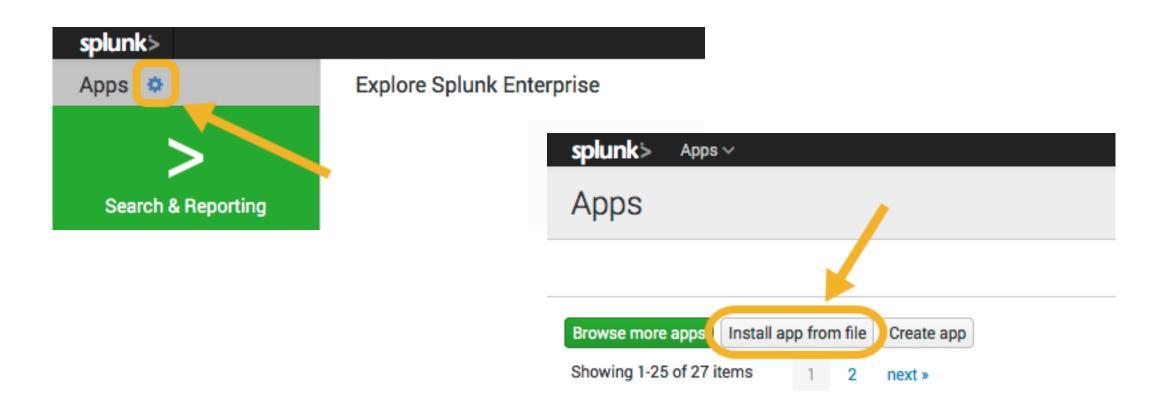
https://splunkbase.splunk.com/app/1620/





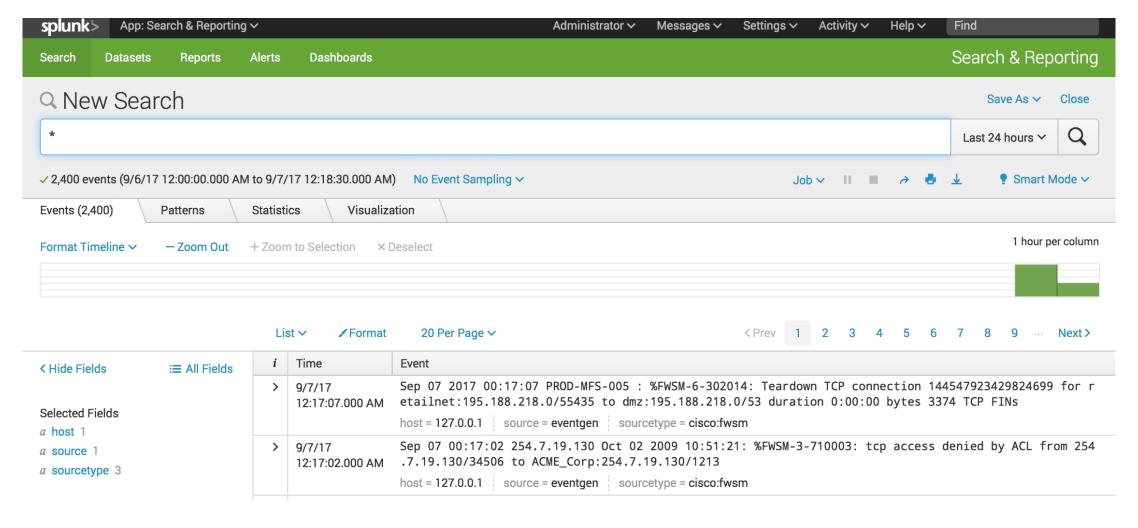
Install The App

Rinse and Repeat





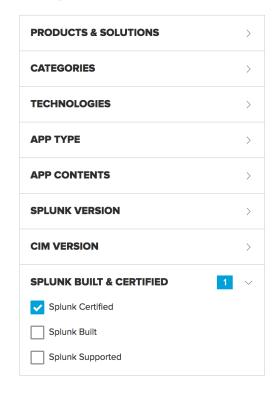
We Have Data



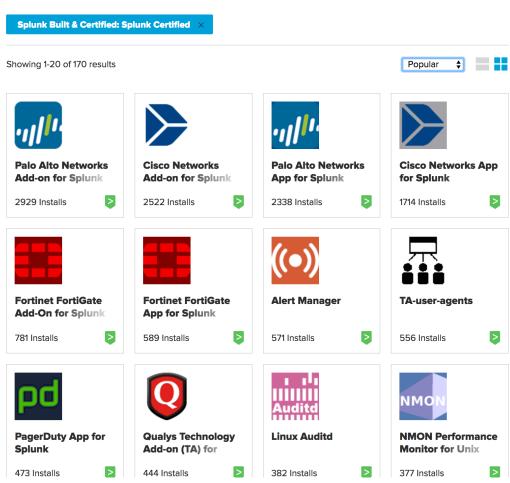


What Apps Work?

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



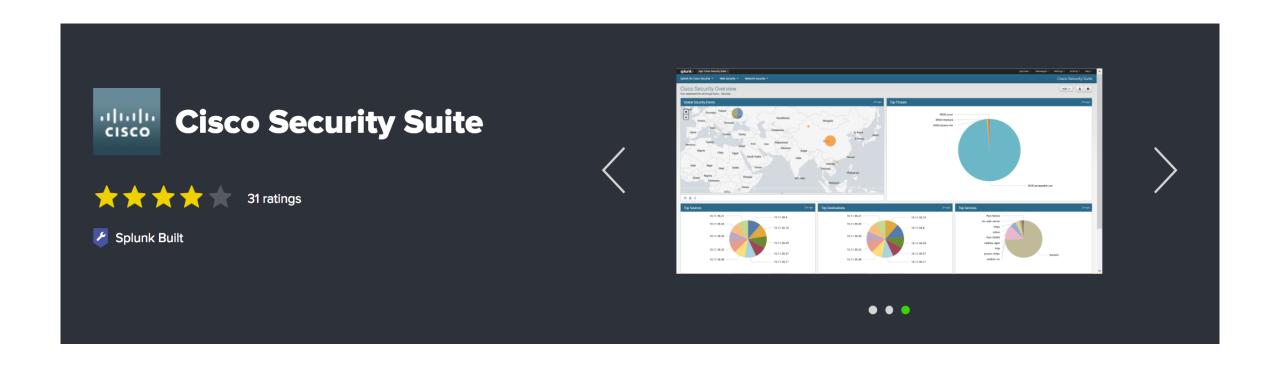
107/Jan 18:10:57:153] "GET / Get / G





What Else Can You Do?

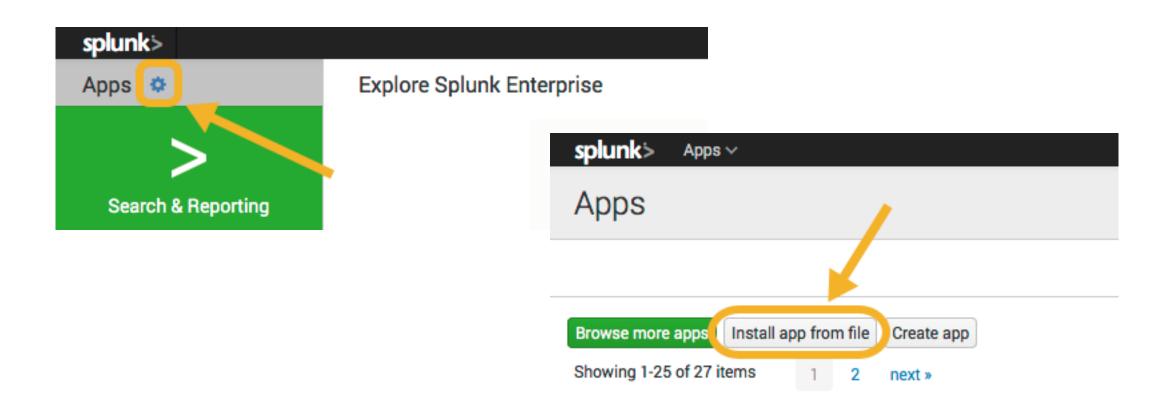
https://splunkbase.splunk.com/app/525/





Install The App

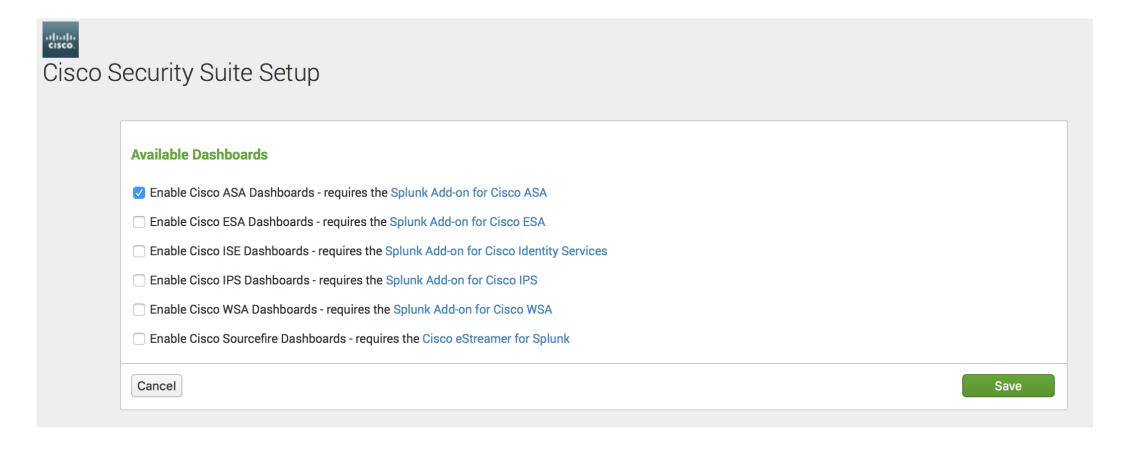
Rinse and Repeat





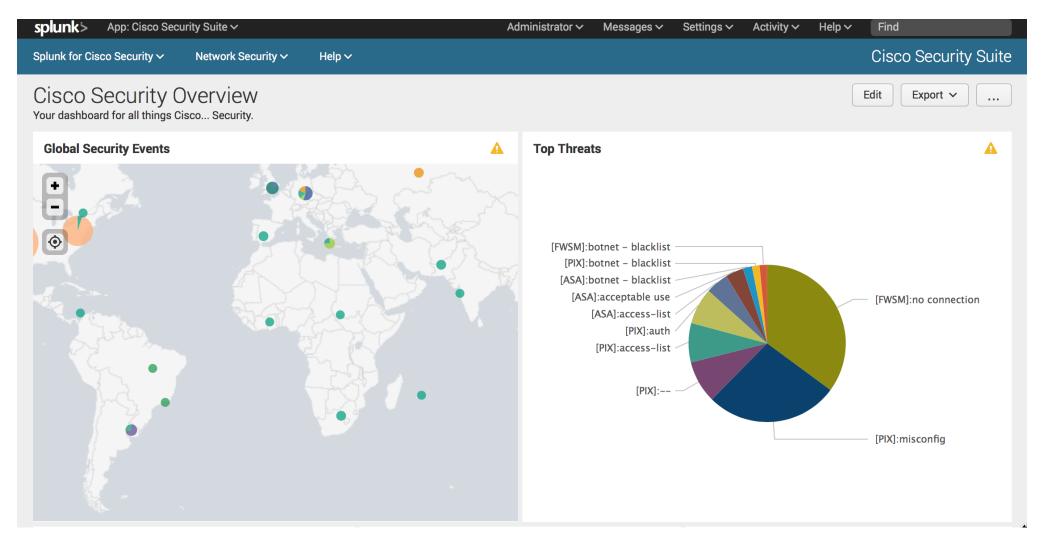
Setup

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





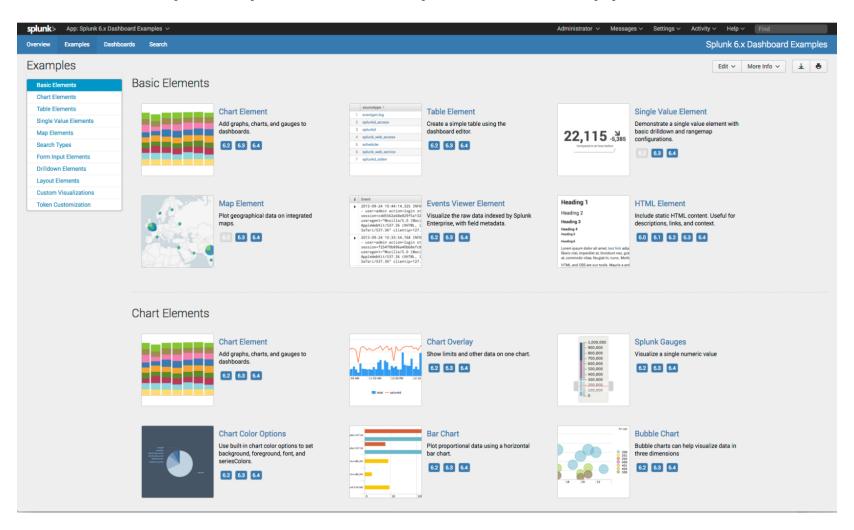
Dashboards!





Splunk 6.x Dashboard Examples

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



. 4310:57:153] "GET /Category.screen?category_id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cattion=purchase&itemid=EST-6&purchase&itemid=EST-8&purchase&itemi



Power of SPL

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

 splunk>
 App: Power of SPL >

 Search
 Walkthrough >
 Dashboards

Table of Contents

Introduction:

This app contains examples of Splunk's Search Processing Language (SPL) that you can use as a tutorial whether you are just getting started with SPL or looking to clicking the links below. Future updates will include more examples and more commands. Happy Splunking!

Data Source:

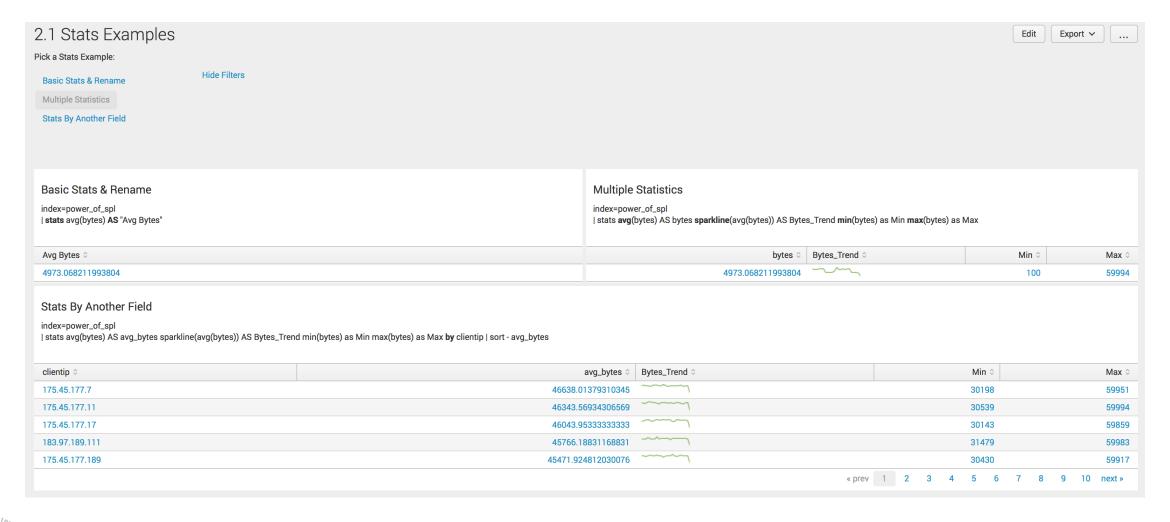
This app comes with a "power_of_spl" index and a static data set containing access_combined logs. All of the searches should begin with index=power_of_spl.

Sections:

- 1. Search and filter + creating/modifying fields Eval
- 2. Charting statistics and predicting values Stats, Sparkline, Timechart, Predict, Trendline, Streamstats, Eventstats
- 3. Converging data sources Lookups, Subsearch, Appendcols
- 4. Mapping Geographic Data Iplocation, Geostats, Geom, Table
- 5. Identifying anomalies Anomalydetection
- 6. Transactions Transaction
- 7. Data exploration & finding relationships between fields Cluster, Fieldsummary, Correlate, Contingency, Analyzefields
- 8. Custom Commands Haversine, Levenshtein, Timewrap



Stats Examples

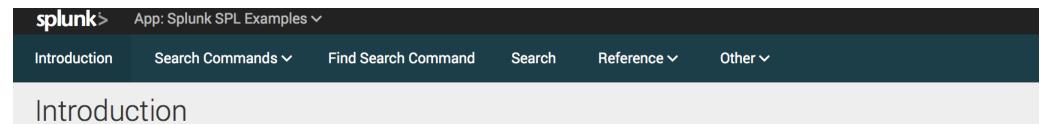


"7'133] "GET /Category.screen?category_id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-lan 18:10:56:123] "GET /product.screen?category_id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-sh. 1.1" 405 322 "http://buttercup-sh. 1.1" 405 322 "http://buttercup-sh. 1.1" 405 322 "http://buttercup-sh. 1.1" 406 322 "http://buttercup-sh. 1.1" 406 322 "http://buttercup-sh. 1.1" 407 322 "http://buttercup-sh. 1.1" 408 322 "http://bu



Splunk SPL Examples

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



Search Processing Language (SPL) Examples for Splunk 6.5.1

The SPL Examples app is designed to take the search reference guide (http://docs.splunk.com/Documentation/Splunk/latest/SearchReference) and show

The data used is mostly based on the tutorial data available from Splunk and some additional data sources

Instructions and notes

This app requires the Splunk Eventgen (https://splunkbase.splunk.com/app/1924/) that can be downloaded from Splunkbase. App the eventgen to your Splunkbase, so the time will vary before all dashbaords are populated.

This app will create 3 new indexes named:

splexamples (25MB)

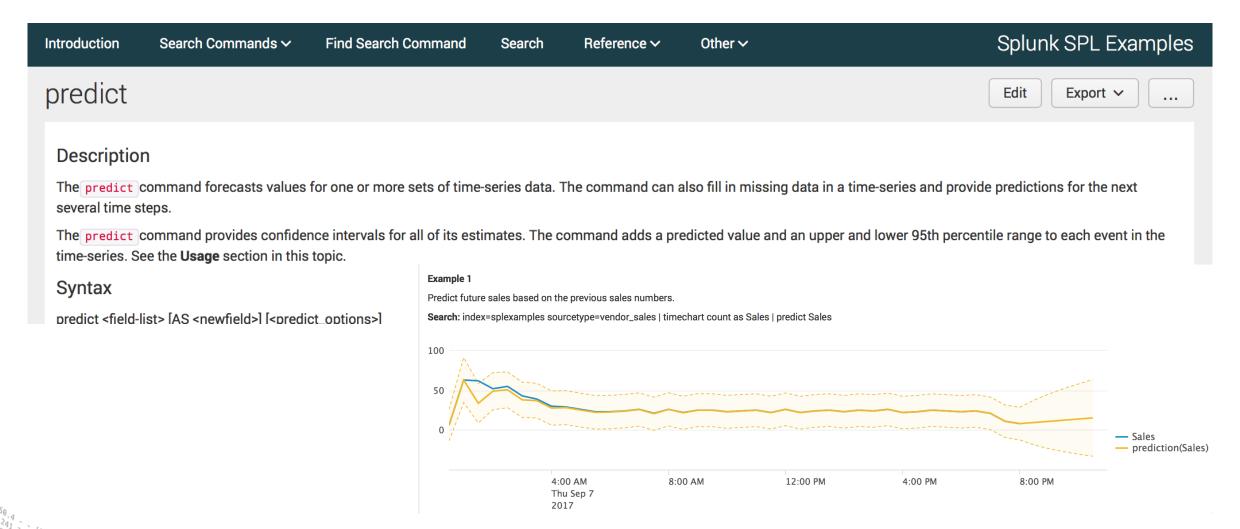
splexamples_downloadcount (1MB)

splexamples_mysummary (1MB)

This app will generate data that will count against your license, this will be less than 25MB per day



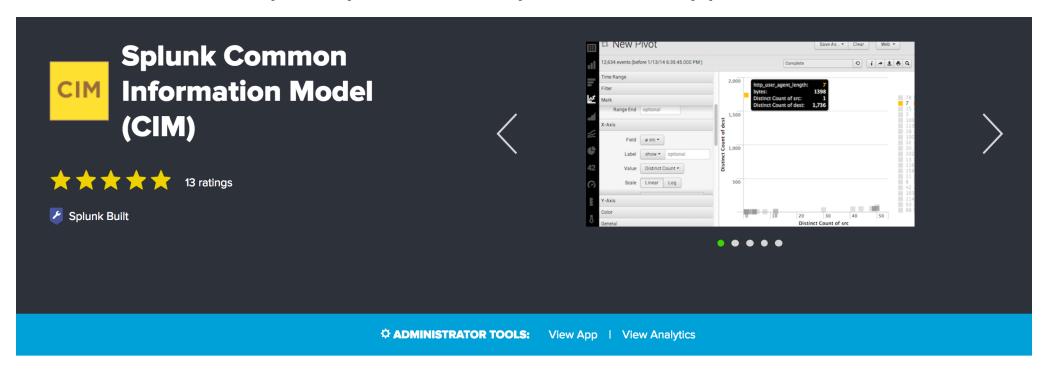
Let's Learn "predict"





Going Beyond

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



Overview Details

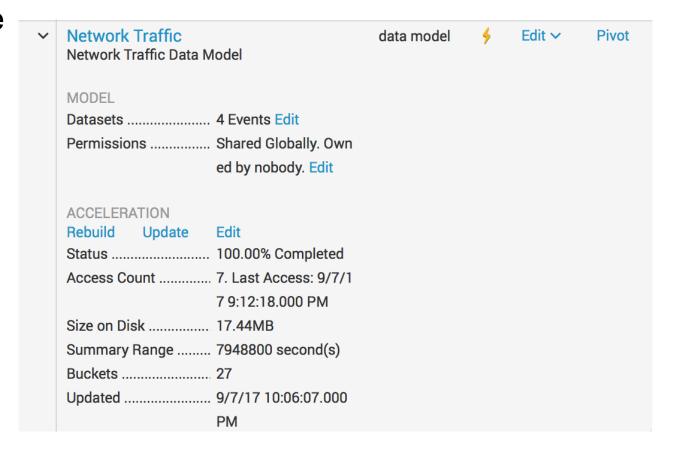
The Common Information Model is a set of field names and tags which are expected to define the least common denominator of a domain of interest. It is implemented as documentation on the Splunk docs website and JSON data model files in this add-on. Use the CIM add-on when modeling data or building apps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





Learn Data Models

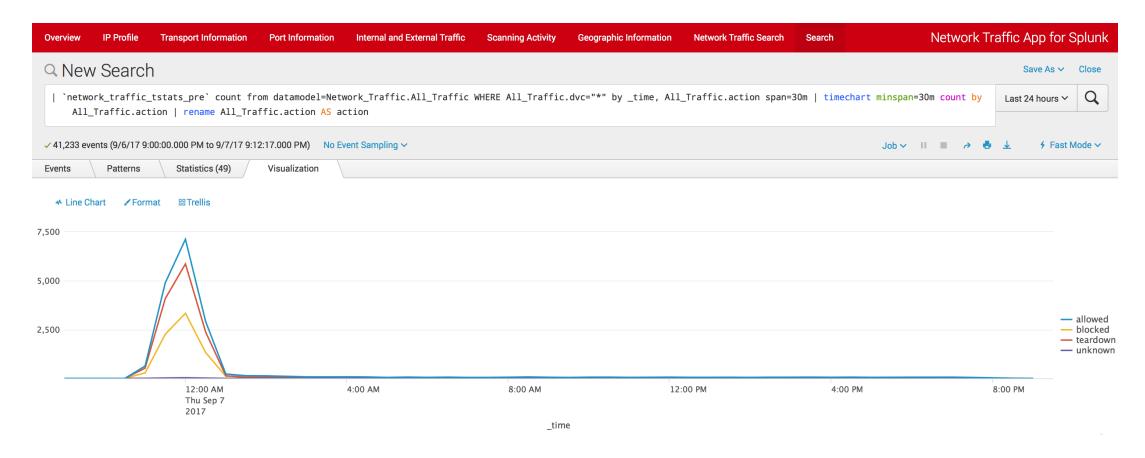
► After installing the CIM app, enable data model acceleration where appropriate and practice tstats and datamodel searches





Network Traffic App for Splunk

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



/product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L7FF6ADFF9 HTTP 1.

/ Old/intracen?product_id=FL-DSH-01&JSESSIONID=SD5L7FF6ADFF9 HTTP 1.1" 200 1318



Keep Your Environment Running

Request a Test/Dev license

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



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

.conf2017

splunk>