

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

130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03"
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
317 27.160.0.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D18SLBFF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03"
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
317 27.160.0.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D18SLBFF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03"
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
317 27.160.0.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D18SLBFF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"

[illegible]

Login

localhost:8000

splunk>enterprise

First time signing in?

If you've forgotten your username or password, please contact your Splunk administrator.

username admin
password changeme

First time signing in?

No Data ☹️

splunk> App: Search & Reporting ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Datasets Reports Alerts Dashboards Search & Reporting

🔍 New Search Save As ▾ Close

* All time ▾ 🔍


✓ 0 events (before 9/6/17 11:50:55.000 PM) No Event Sampling ▾ Job ▾ || ■ ➔ 🖨 ⬇ 💡 Smart Mode ▾

Events (0) Patterns Statistics Visualization


❗ No results found.


Download Eventgen


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




Search App by keyword, technology...


 My Account ▾

 My Splunk ▾


 Support & Services ▾



Eventgen

 8 ratings

<https://goo.gl/bc3eF9>

 **ADMINISTRATOR TOOLS:** [View App](#)

Overview

Details

Eventgen allows an app developer to describe, through configuration or code, events to generate. This allows an app developer to get events into Splunk to test their applications.

5,812

Downloads

[Visit Site](#)

[Rate this App](#)

Install The App

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



130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03" "Mozilla/4.0" "Opera/9.20" "Computer" "Win" "128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/4.0" "Computer" "Win" "317.27.160.0.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D18SL8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/4.0" "Computer" "Win" "130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03" "Mozilla/4.0" "Opera/9.20" "Computer" "Win" "128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/4.0" "Computer" "Win" "317.27.160.0.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D18SL8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/4.0" "Computer" "Win"

Upload An App

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

Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. [Learn more.](#)

File

Browse... No file selected.

☐ Upgrade app. Checking this will overwrite the app if it already exists.

Cancel

Upload

Restart Splunk

Restart Required

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

[Restart Later](#)[Restart Now](#)

Still No Data ☹️

splunk> App: Search & Reporting ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Datasets Reports Alerts Dashboards Search & Reporting

🔍 New Search Save As ▾ Close

* All time ▾ 🔍







✓ 0 events (before 9/6/17 11:50:55.000 PM) No Event Sampling ▾ Job ▾ ⏸ ■ ➡ 🖨 ⬇ 💡 Smart Mode ▾

Events (0) Patterns Statistics Visualization

⚠️ No results found.







Where do you get Apps? Splunkbase!

Browse by Category

 DevOps 41 Apps	 IT Operations 634 Apps	 Security, Fraud & Compliance 572 Apps
 Business Analytics 94 Apps	 IoT & Industrial Data 75 Apps	 Utilities 565 Apps







Browse by Technology

[See all Cisco apps >](#)

CISCO		DELL EMC		amazon web services		paloalto NETWORKS	
	Cisco Networks App for Splunk Enterprise 1661 Installs		Splunk Add-on for Cisco UCS 223 Installs		TA-meraki 183 Installs		Cisco ACI Add-on for Splunk Enterprise 88 Installs
	Cisco AnyConnect Network Visibility 85 Installs		Cisco ACI App for Splunk Enterprise 83 Installs				


Splunk Built Apps

[See all apps >](#)


	Splunk UBA RHEL 7.2 Software for Bare		Splunk UBA RHEL 6.7 Software for Bare		Splunk App for PCI Compliance - Splunk		Splunk UBA OVA Software		Splunk UBA Software Update		Splunk IT Service Intelligence
---	--	---	--	---	---	---	--------------------------------	---	-----------------------------------	---	---------------------------------------

How About This One?


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



Splunk Add-on for Cisco ASA



8 ratings



Splunk Built

4,748

Installs

Download

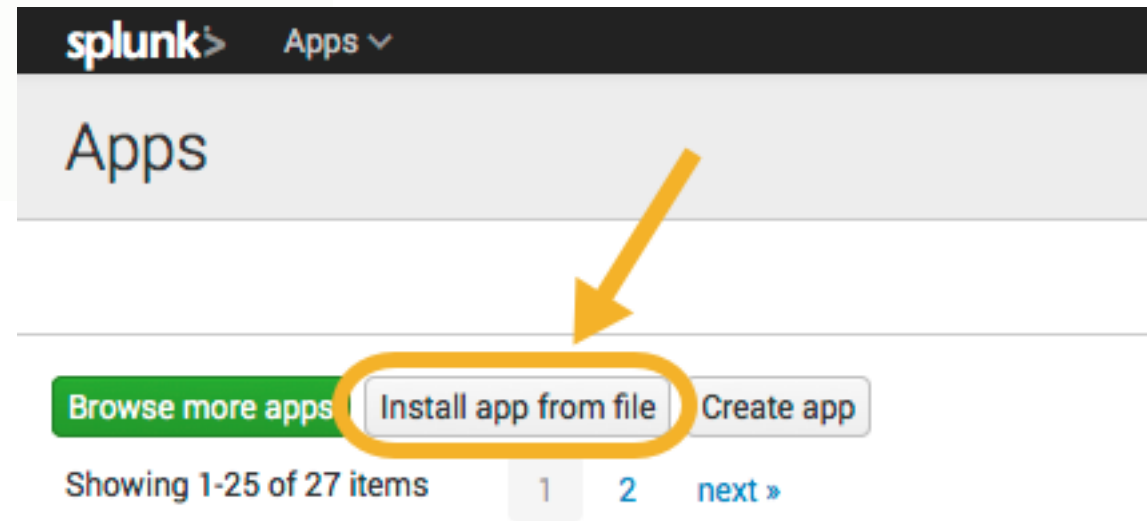
34,672

Downloads

Rate this App

Install The App

Rinse and Repeat



We Have Data ☺

splunk> App: Search & Reporting ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Datasets Reports Alerts Dashboards Search & Reporting

🔍 New Search Save As ▾ Close

* Last 24 hours ▾ 🔍

✓ 2,400 events (9/6/17 12:00:00.000 AM to 9/7/17 12:18:30.000 AM) No Event Sampling ▾ Job ▾ ⏏ 📄 ⬇ 💡 Smart Mode ▾

Events (2,400) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 hour per column

List ▾ 🔧 Format 20 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 9 ... Next >

< Hide Fields ☰ All Fields

Selected Fields
a host 1
a source 1
a sourcetype 3

i	Time	Event
>	9/7/17 12:17:07.000 AM	Sep 07 2017 00:17:07 PROD-MFS-005 : %FWSM-6-302014: Teardown TCP connection 144547923429824699 for retailnet:195.188.218.0/55435 to dmz:195.188.218.0/53 duration 0:00:00 bytes 3374 TCP FINs host = 127.0.0.1 source = eventgen sourcetype = cisco:fwsm
>	9/7/17 12:17:02.000 AM	Sep 07 00:17:02 254.7.19.130 Oct 02 2009 10:51:21: %FWSM-3-710003: tcp access denied by ACL from 254.7.19.130/34506 to ACME_Corp:254.7.19.130/1213 host = 127.0.0.1 source = eventgen sourcetype = cisco:fwsm

What Apps Work?

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

PRODUCTS & SOLUTIONS >

CATEGORIES >

TECHNOLOGIES >

APP TYPE >

APP CONTENTS >

SPLUNK VERSION >

CIM VERSION >


SPLUNK BUILT & CERTIFIED 1 v

☒ Splunk Certified
 ☐ Splunk Built
 ☐ Splunk Supported

Splunk Built & Certified: Splunk Certified x


Showing 1-20 of 170 results

Popular




Palo Alto Networks Add-on for Splunk

2929 Installs




Cisco Networks Add-on for Splunk

2522 Installs




Palo Alto Networks App for Splunk

2338 Installs




Cisco Networks App for Splunk

1714 Installs




Fortinet FortiGate Add-On for Splunk

781 Installs




Fortinet FortiGate App for Splunk

589 Installs




Alert Manager

571 Installs




TA-user-agents

556 Installs




PagerDuty App for Splunk

473 Installs




Qualys Technology Add-on (TA) for

444 Installs



Linux Auditd

382 Installs



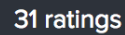
NMON Performance Monitor for Unix

377 Installs

splunk> .conf2017

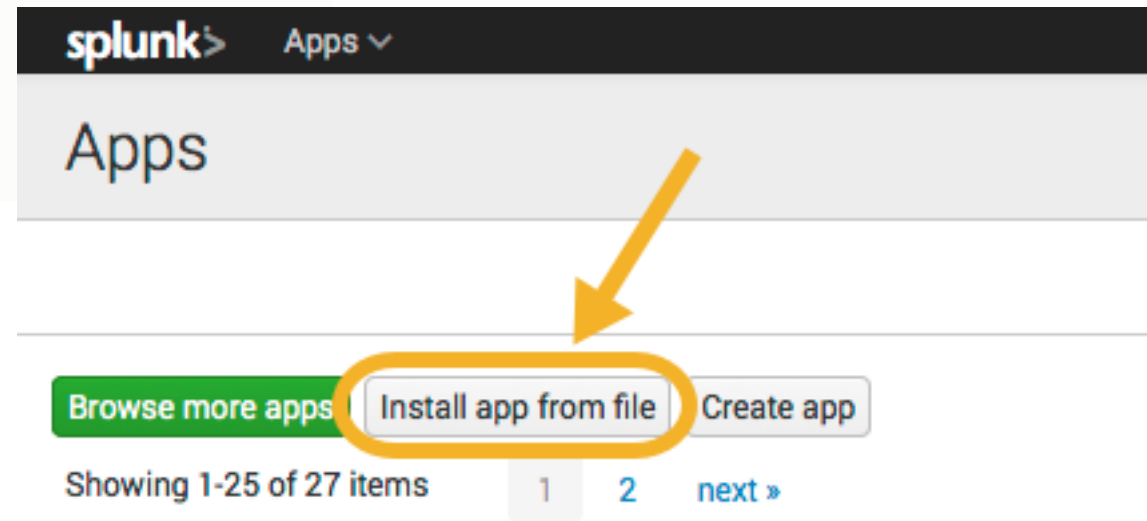
<https://splunkbase.splunk.com/app/525/>

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



Install The App

Rinse and Repeat



Setup

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



Cisco Security Suite Setup

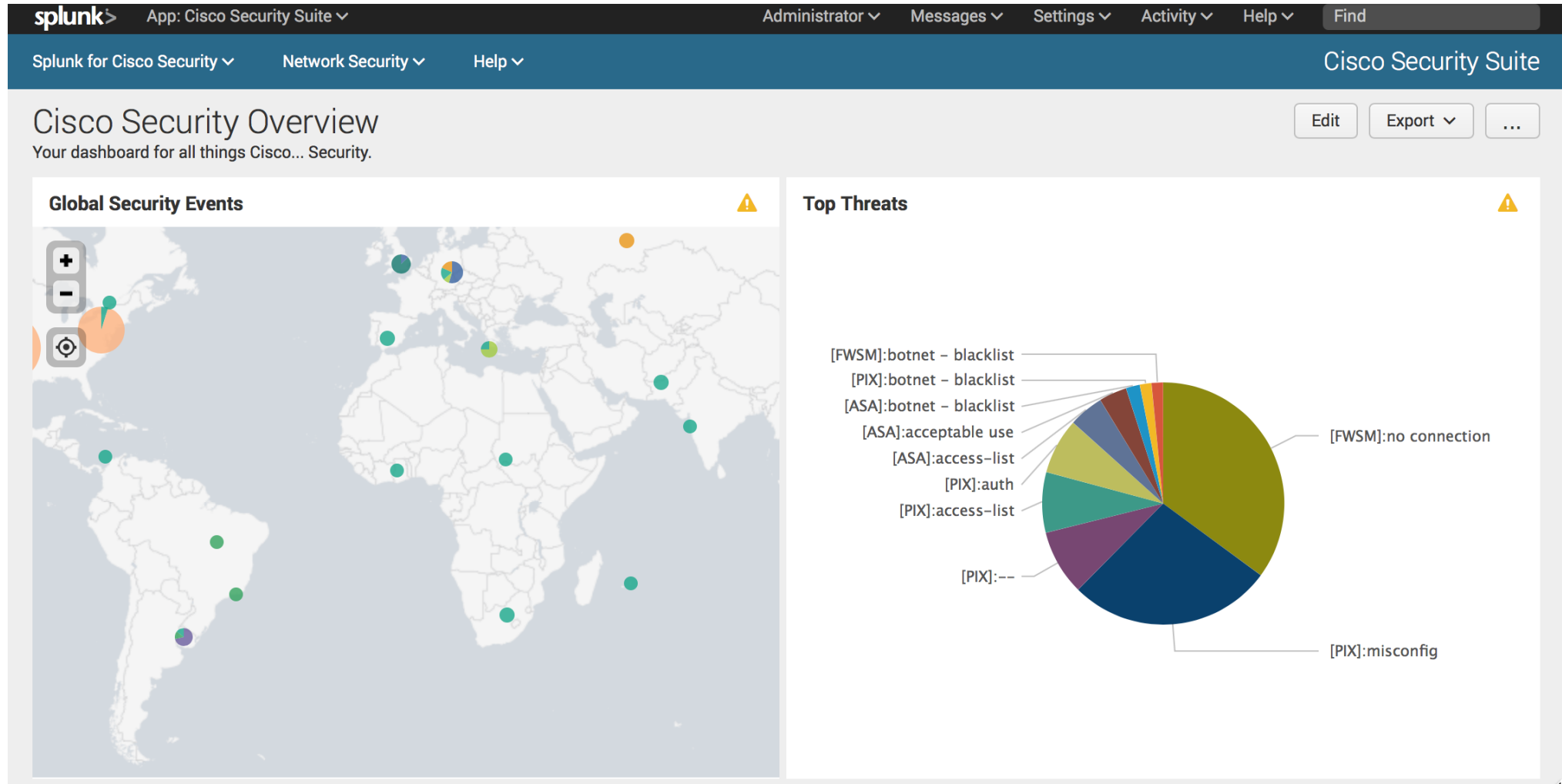
Available Dashboards

- ☒ Enable Cisco ASA Dashboards - requires the [Splunk Add-on for Cisco ASA](#)
- ☐ Enable Cisco ESA Dashboards - requires the [Splunk Add-on for Cisco ESA](#)
- ☐ Enable Cisco ISE Dashboards - requires the [Splunk Add-on for Cisco Identity Services](#)
- ☐ Enable Cisco IPS Dashboards - requires the [Splunk Add-on for Cisco IPS](#)
- ☐ Enable Cisco WSA Dashboards - requires the [Splunk Add-on for Cisco WSA](#)
- ☐ Enable Cisco Sourcefire Dashboards - requires the [Cisco eStreamer for Splunk](#)

Cancel

Save

Dashboards!



Splunk 6.x Dashboard Examples

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

splunk> App: Splunk 6.x Dashboard Examples

Administrator Messages Settings Activity Help Find

Overview Examples Dashboards Search

Splunk 6.x Dashboard Examples

Edit More Info

Examples

- Basic Elements
- Chart Elements
- Table Elements
- Single Value Elements
- Map Elements
- Search Types
- Form Input Elements
- Drilldown Elements
- Layout Elements
- Custom Visualizations
- Token Customization

Basic Elements

Chart Element
Add graphs, charts, and gauges to dashboards.
6.2 6.3 6.4


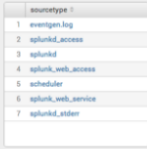




Table Element
Create a simple table using the dashboard editor.
6.2 6.3 6.4



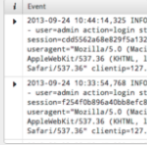
Single Value Element
Demonstrate a single value element with basic drilldown and rangemap configurations.
6.2 6.3 6.4



Map Element
Plot geographical data on integrated maps.
6.2 6.3 6.4



Events Viewer Element
Visualize the raw data indexed by Splunk Enterprise, with field metadata.
6.2 6.3 6.4



Heading 1
Heading 2
Heading 3
Heading 4
Heading 5

HTML Element
Include static HTML content. Useful for descriptions, links, and context.
6.0 6.1 6.2 6.3 6.4




Chart Elements

Chart Element
Add graphs, charts, and gauges to dashboards.
6.2 6.3 6.4





Chart Overlay
Show limits and other data on one chart.
6.2 6.3 6.4



Splunk Gauges
Visualize a single numeric value
6.2 6.3 6.4

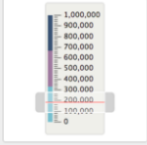




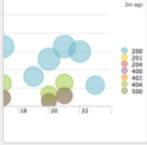
Chart Color Options
Use built-in chart color options to set background, foreground, font, and series colors.
6.2 6.3 6.4



Bar Chart
Plot proportional data using a horizontal bar chart.
6.2 6.3 6.4



Bubble Chart
Bubble charts can help visualize data in three dimensions
6.2 6.3 6.4



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 - [Ilocation](#), [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

2.1 Stats Examples

Edit

Export ▾

...

Pick a Stats Example:

Basic Stats & Rename

Hide Filters

Multiple Statistics

Stats By Another Field

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 »

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

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

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.

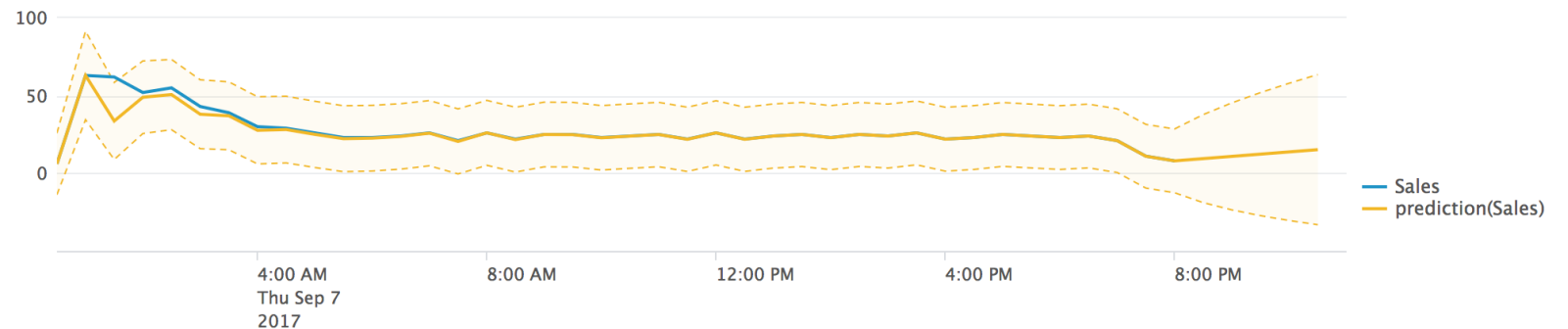
Syntax

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

Example 1


Predict future sales based on the previous sales numbers.

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




Going Beyond

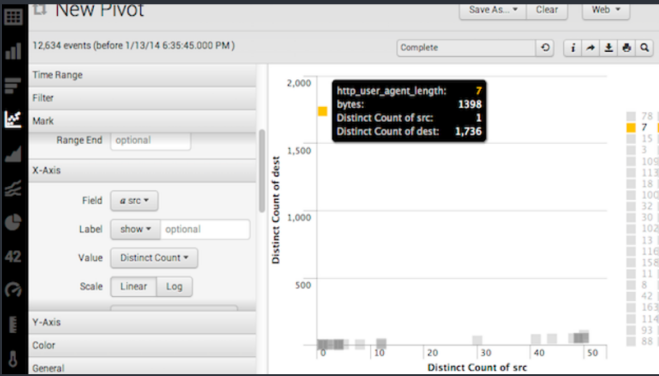
<https://splunkbase.splunk.com/app/1621/>



Splunk Common Information Model (CIM)

★★★★★ 13 ratings

 Splunk Built



ADMINISTRATOR TOOLS: [View App](#) | [View Analytics](#)

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

[Download](#)

28,683

Downloads

[Rate this App](#)

splunk>

.conf2017

- 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>

[Overview](#) [IP Profile](#) [Transport Information](#) [Port Information](#) [Internal and External Traffic](#) [Scanning Activity](#) [Geographic Information](#) [Network Traffic Search](#) [Search](#) **Network Traffic App for Splunk**

New Search

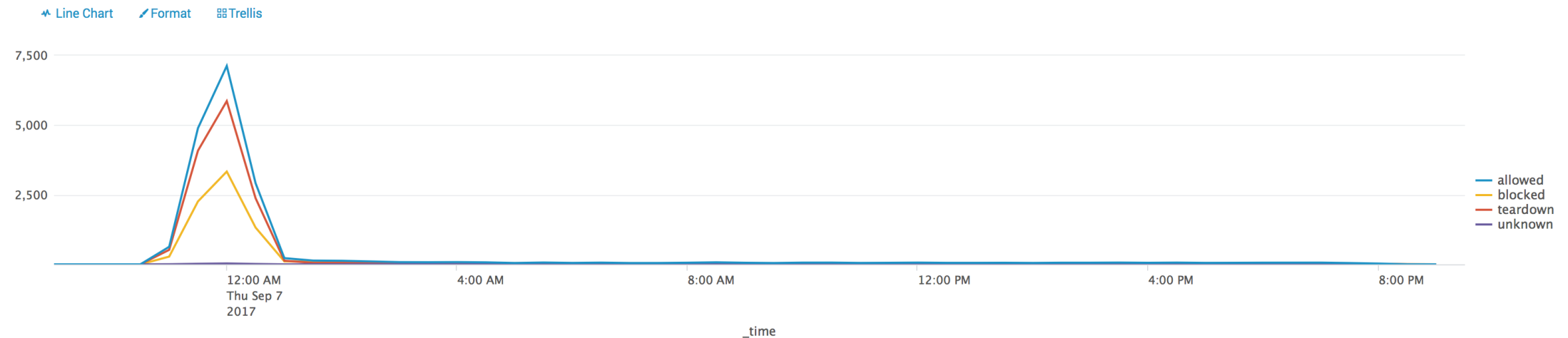
| `network_traffic_tstats_pre` count from datamodel=Network_Traffic.All_Traffic WHERE All_Traffic.dvc="*" by _time, All_Traffic.action span=30m | timechart minspan=30m count by All_Traffic.action | rename All_Traffic.action AS action

Save As ▾ Close

Last 24 hours ▾

✓ 41,233 events (9/6/17 9:00:00.000 PM to 9/7/17 9:12:17.000 PM) [No Event Sampling ▾](#) [Job ▾](#) Fast Mode ▾

[Events](#) [Patterns](#) [Statistics \(49\)](#) [Visualization](#)



Keep Your Environment Running

Request a Test/Dev license

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

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D3SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D18SLBFF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D3SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D18SLBFF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D3SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D18SLBFF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"

► Check out gogen, made by the same author as eventgen

- ▶ Fake-factory, a Python library

- ## ► 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

splunk> .conf2017