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
No Data 😞
Download Eventgen
https://splunkbase.splunk.com/app/1924/

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.
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 Required

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

Restart Later  Restart Now
Still No Data 😞
Let’s Grab an App
Where do you get Apps? Splunkbase!
How About This One?
https://splunkbase.splunk.com/app/1620/

Splunk Add-on for Cisco ASA

4,748 Installs
34,672 Downloads
Install The App
Rinse and Repeat
We Have Data 😊
What Apps Work?
Anything that is Splunk certified and/or has an eventgen.conf file!
What Else Can You Do?
https://splunkbase.splunk.com/app/525/

Cisco Security Suite

★ ★ ★ ★ ★ 31 ratings

Splunk Built
Install The App
Rinse and Repeat
Setup
Since we’ve only installed the Add-on for Cisco ASA

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

Save
Cancel
Dashboards!
Splunk 6.x Dashboard Examples
https://splunkbase.splunk.com/app/1603/
Power of SPL
https://splunkbase.splunk.com/app/3353/

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

#### Basic Stats & Rename

```
index=power_of_spl
| stats avg(bytes) AS 'Avg Bytes'
```

<table>
<thead>
<tr>
<th>Avg Bytes</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>4973.068211993864</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Multiple Statistics

```
index=power_of_spl
| stats avg(bytes) AS sparkline(avg(bytes)) A5 Bytes_Trend min(bytes) as Min max(bytes) as Max
```

<table>
<thead>
<tr>
<th>byte</th>
<th>Bytes_Trend</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>4973.068211993804</td>
<td></td>
<td>100</td>
<td>59994</td>
</tr>
</tbody>
</table>

#### Stats By Another Field

```
index=power_of_spl
| stats avg(bytes) AS avg_bytes sparkline(avg(bytes)) A5 Bytes_Trend min(bytes) as Min max(bytes) as Max by clientip | sort: avg_bytes
```

<table>
<thead>
<tr>
<th>clientip</th>
<th>avg_bytes</th>
<th>Bytes_Trend</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>175.45.177.7</td>
<td>46638.01379310245</td>
<td></td>
<td>30198</td>
<td>59951</td>
</tr>
<tr>
<td>175.45.177.11</td>
<td>46343.56934305659</td>
<td></td>
<td>30539</td>
<td>59994</td>
</tr>
<tr>
<td>175.45.177.17</td>
<td>46043.95333333333</td>
<td></td>
<td>30143</td>
<td>59859</td>
</tr>
<tr>
<td>183.97.185.111</td>
<td>45763.18831168831</td>
<td></td>
<td>31479</td>
<td>59983</td>
</tr>
<tr>
<td>175.45.177.189</td>
<td>45471.924812030076</td>
<td></td>
<td>30430</td>
<td>59917</td>
</tr>
</tbody>
</table>
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 Splunk backfill process, so the time will vary before all dashboards 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”

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]`
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.
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
Keep Your Environment Running
Request a Test/Dev license

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)

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