Splunk and the Weather
Powered by the Dark Sky API

Somen De | Function1

September 27, 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.
About Function1
www.function1.com

- Founded in 2007; offices in Washington D.C., New York City, Toronto, and Chicago
- One of Splunk’s premier professional services partners
- More than 1,000 successful Splunk engagements spanning all industry verticals: Security, Finance, Energy, E-Commerce, Government, Defense, Healthcare, Entertainment, Retail, and Education
- Our team of Splunk experts is credited with designing the base architecture for some of the largest Splunk deployments to-date and have aided in developing the standard for enterprise class governance and data onboarding
“Climate Is What We Expect, Weather Is What We Get.”

- Mark Twain
At Function1, we blog quarterly and are encouraged to find new and exciting ways to utilize Splunk.
Dark Sky API
Quick Overview

▶ The Dark Sky API allows you to look up the weather anywhere on the globe, returning (where available):

• Current weather conditions
• Minute-by-Minute forecasts out to one hour
• Hour-by-hour and day-by-day forecasts out to seven days
• Hour-by-hour and day-by-day observations going back decades

▶ They provide two types of API requests:

• A Forecast Request returns the current weather forecast for the next week in JSON format.
• A Time Machine Request returns the observed or forecast weather conditions for a date in the past or future in the same JSON format.
Data can be historical or from the future!
- Anytime in the past or future
- Just pass in an epoch time variable

Data can be searched and charted in intervals
- Currently
- Daily
- Hourly
- Minutely

Data is returned in neat and clean JSON
- props.conf
Visualize Weather Trends
Max Temperature vs Min Temperature, per day, over 1 year
Lower Manhattan
Visualize Weather Trends
Precipitation Intensity, Summer 2016
Lower Manhattan

Average Precipitation Intensity over Time

index="weather_json" | timechart span=3d avg("daily.data().precipIntensity")

308 events (5/1/16 12:00:00.000 AM to 10/2/16 12:00:00.000 AM) No Event Sampling

Events   Patterns   Statistics (52)   Visualization

Area Chart   Format   Trellis

Avg Precipitation Intensity

Sun May 1 2016   Sat May 28   Fri Jun 24   Thu Jul 21   Wed Aug 17
Visualize Weather Trends
Average Wind Speed, per day, October 2016
Lower Manhattan
The Dark Sky API offers fields that Splunk can utilize to forecast Rain

- Dewpoint
- Humidity
- Pressure
- Cloud Cover

We also set up a simple "eval" to create a field that we run the prediction on

- eval rain=if(LIKE(summary,"%Rain%"),"rain","norain")
Predict the Weather!
Use the Splunk Machine Learning Toolkit

Predict Categorical Fields
Predict the value of a categorical field using the values of other fields in that event.

Create New Model

Enter a search

```
index=conf
| eval rain=if(LIKE(summary,"%Rain%"),"rain","norain")
```

10,267 events (3/1/16 12:00:00.000 AM to 9/10/17 6:40:46.000 PM)

Preprocessing Steps
No steps added.

+ Add a step

Algorithm: GaussianNB
Field to predict: rain
Fields to use for predicting: dewPoint, humidity, pressure, cloudCover

Save the model as: default_model_name

Split for training / test: 60 / 40
## Predict the Weather!
Use the Splunk Machine Learning Toolkit

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precision</td>
<td>0.94</td>
</tr>
<tr>
<td>Recall</td>
<td>0.93</td>
</tr>
<tr>
<td>Accuracy</td>
<td>0.93</td>
</tr>
<tr>
<td>F1</td>
<td>0.93</td>
</tr>
</tbody>
</table>
Thank You

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