splunk> .conf2017

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.

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
- Services: Installation & Upgrades, Data Onboarding, Training, Dashboard & App Development, Products, Health Checks, Consulting
- 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

CIOReview

America's Fastest-Growing Private Companies Inc. 5000

USPAACC Fast 100 Asian American Business

GREAT PLACE TO WORK®

“Climate Is What We Expect, Weather Is What We Get.”

- Mark Twain

Splunk - Function1 - Dark Sky API

- At Function1, we blog quarterly and are encouraged to find new and exciting ways to utilize Splunk

splunk> function1 Powered by Dark Sky

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.

Dark Sky API

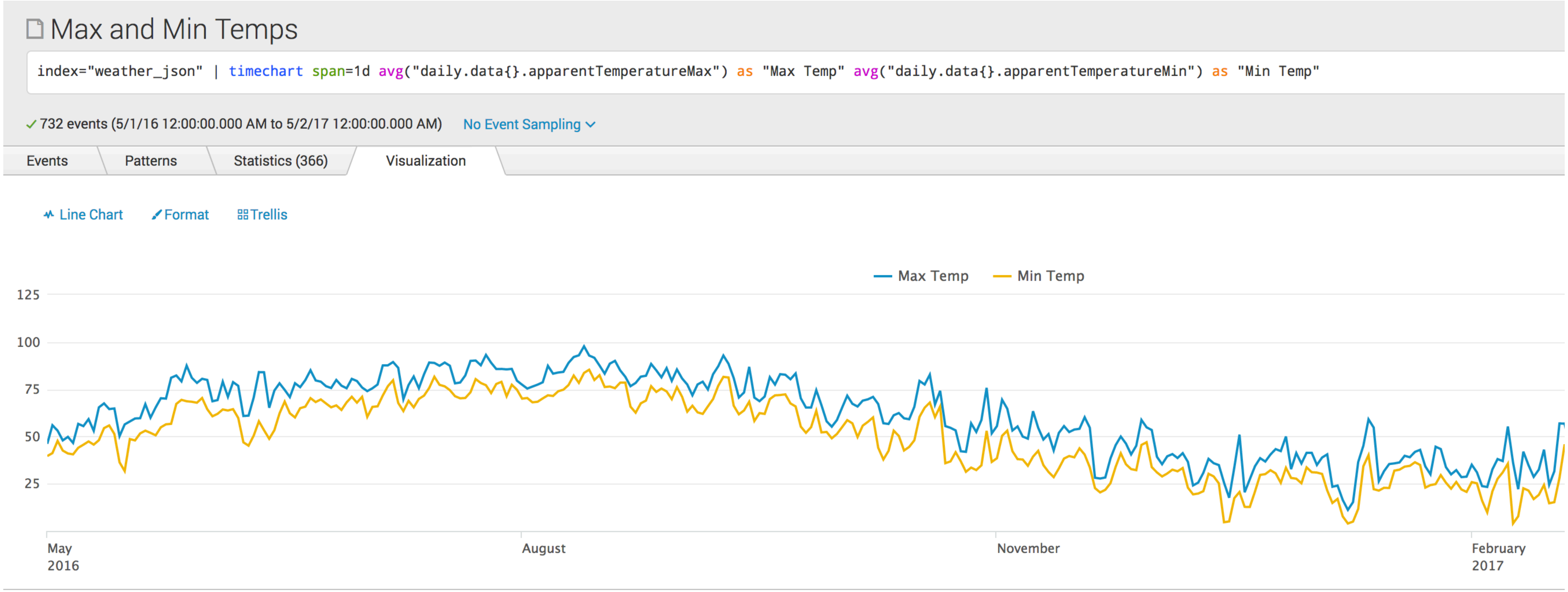
Why it's Perfect for Splunk

- 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



Max and Min Temps

```
index="weather_json" | timechart span=1d avg("daily.data{}.apparentTemperatureMax") as "Max Temp" avg("daily.data{}.apparentTemperatureMin") as "Min Temp"
```

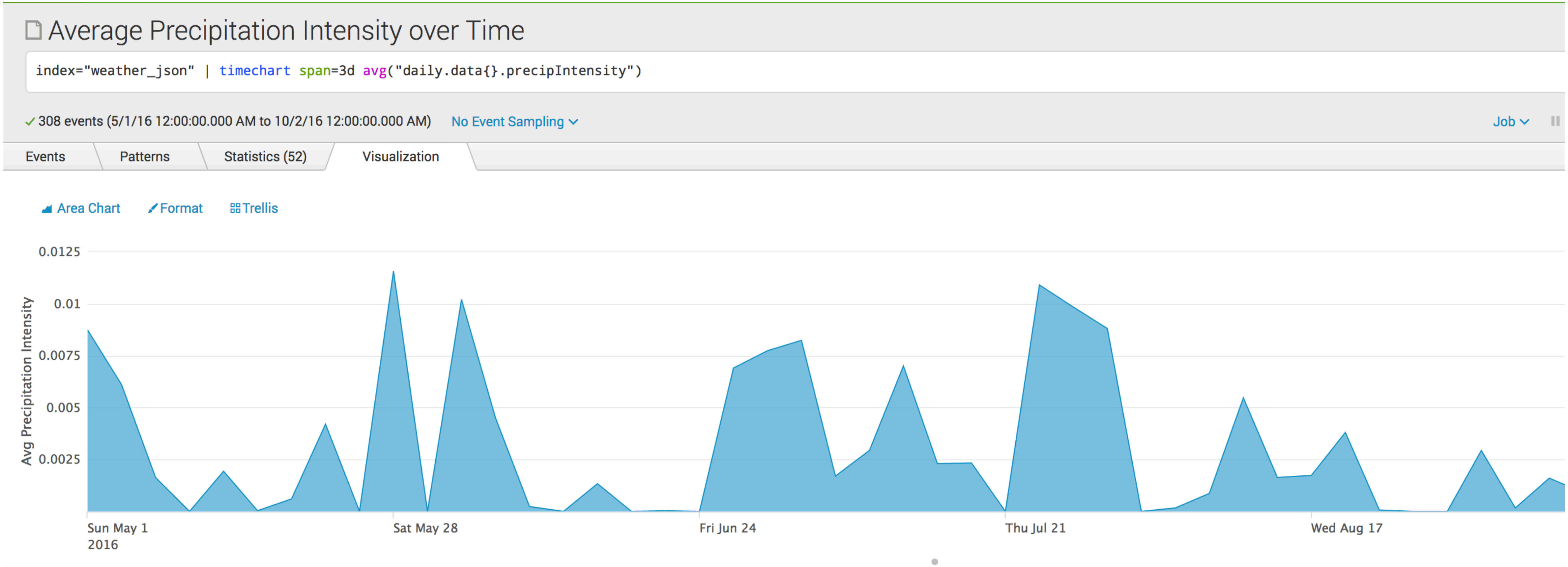
✓ 732 events (5/1/16 12:00:00.000 AM to 5/2/17 12:00:00.000 AM)

splunk> .conf2017

Visualize Weather Trends

Precipitation Intensity, Summer 2016

Lower Manhattan



Average Precipitation Intensity over Time

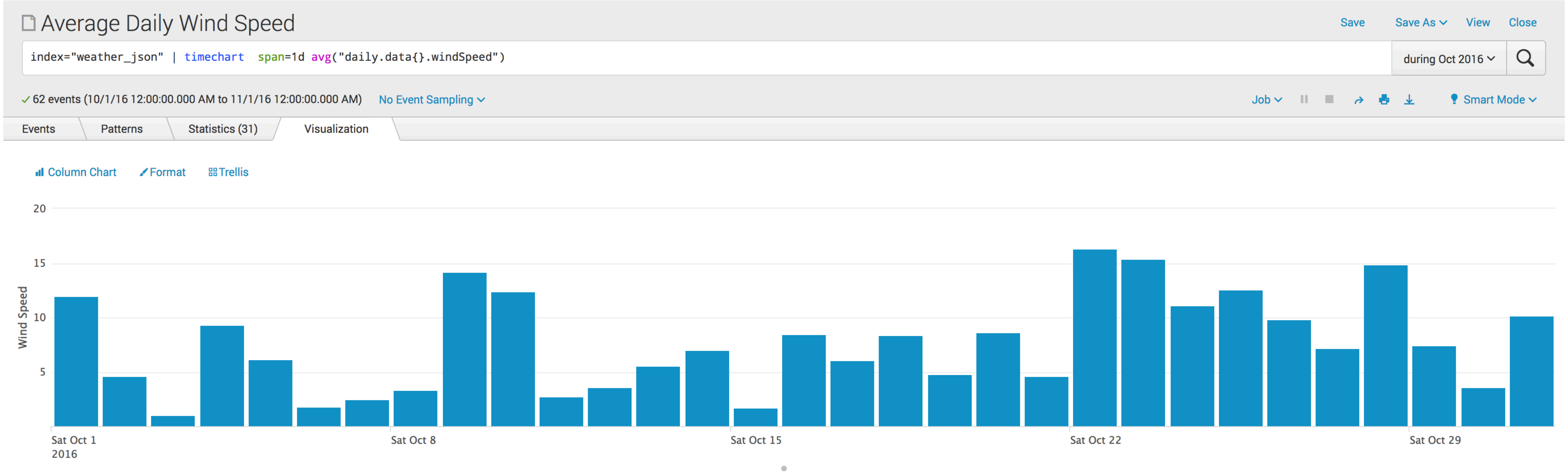
```
index="weather_json" | timechart span=3d avg("daily.data{}.precipIntensity")
```

✓ 308 events (5/1/16 12:00:00.000 AM to 10/2/16 12:00:00.000 AM)

Visualize Weather Trends

Average Wind Speed, per day, October 2016

Lower Manhattan



Average Daily Wind Speed

```
index="weather_json" | timechart  span=1d avg("daily.data{}.windSpeed")
```

during Oct 2016

✓ 62 events (10/1/16 12:00:00.000 AM to 11/1/16 12:00:00.000 AM)

No Event Sampling

Predict the Weather!

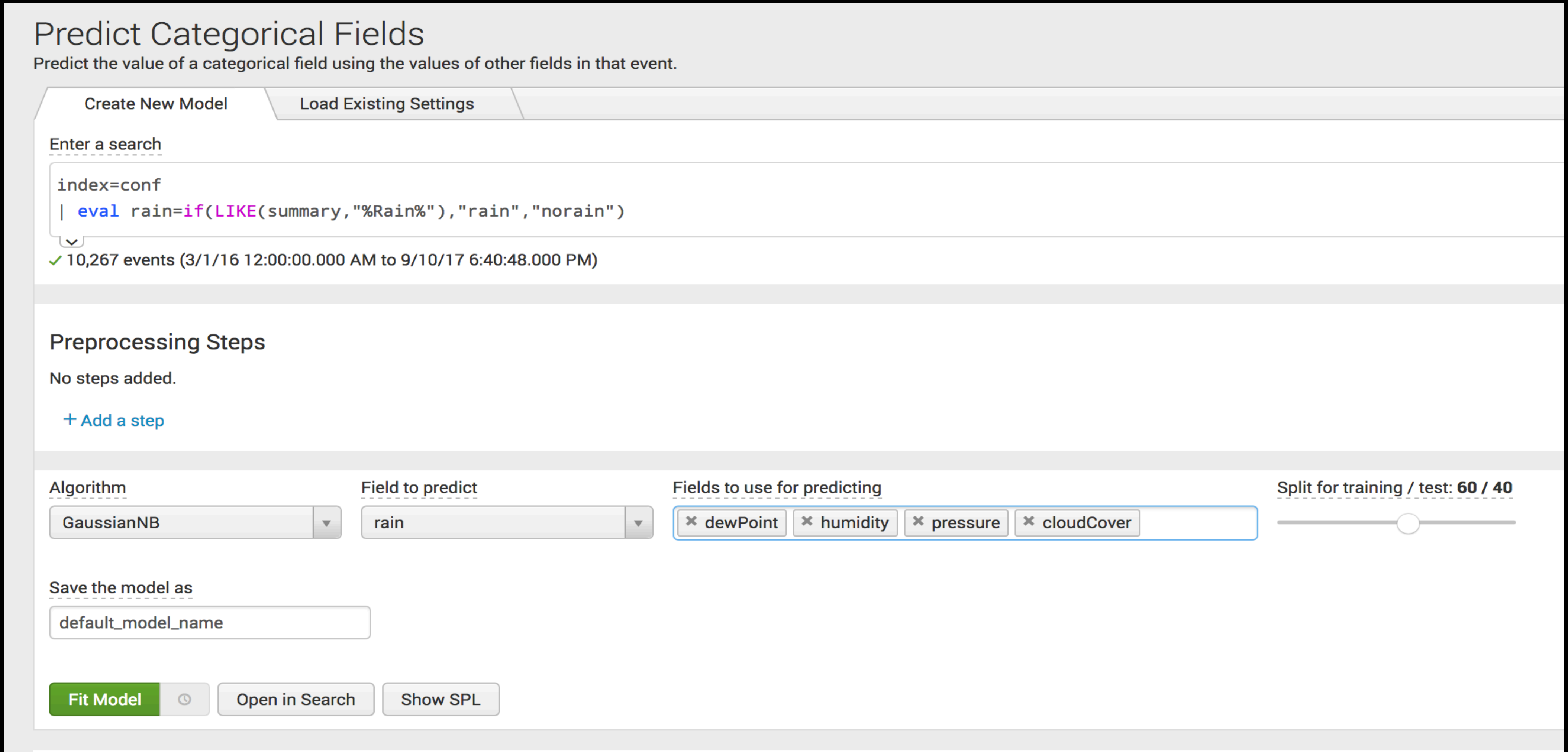
How Can We Predict if it will Rain?

- 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.

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 6:40:48.000 PM)

Preprocessing Steps

No steps added.

Algorithm: GaussianNB

Field to predict: rain

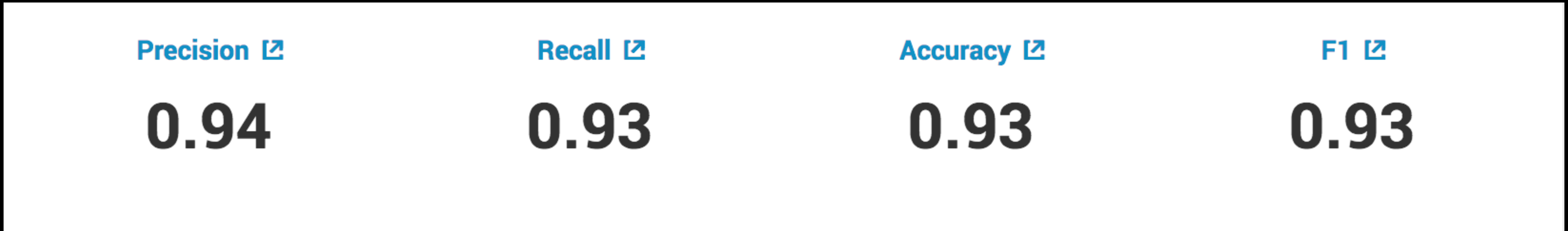
Fields to use for predicting: dewPoint, humidity, pressure, cloudCover

Split for training / test: **60 / 40**

Save the model as: default_model_name

Predict the Weather!

Use the Splunk Machine Learning Toolkit



Precision	Recall	Accuracy	F1
0.94	0.93	0.93	0.93

Thank You

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

splunk> .conf2017