Splunk This! - Bringing Natural Language Processing To Splunk

Dipock Das | Incubation Projects

September 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.
Making machine data accessible, usable and valuable to everyone.
Machine Data

Internal  Enterprise  External
Example: Retail Store

Internal
- Point of sale, SKU, Inventory, Labour, Sales, Returns, Loss, Utilities, Customers, Payments, Sensors

Enterprise
- Warehouse, Deliveries, Shipping, Marketing, Surveys, Facilities, Regional Totals, Manufacturing, Supply Chain, Security, Recalls, DMA, Competition

External
- Weather, Social Media, Traffic, Demographics, Legislation, Aircraft arrivals and departures, Exchange rates, Sporting Events, Public Events, Holidays
Delivers Actionable Operational Insights

- Internal
- Enterprise
- External

Splunk Machine learning

Splunk

Yo!
“Everyone..”

New Industries And Personas

- Energy
- Commerce
- Transportation
- Retail
- Manufacturing
- Food Service
Data ... is all over the place
You need training and Ninja skills ...
What if you could interact with your data without the skills?
Splunk Data Fabric + Natural Language Processing

Web
Mobile
Voice
API

splunk>enterprise

splunk>cloud

splunk> Platform for Operational Intelligence

Syslog/TCP
Network Wire Data
Mobile
IoT Devices
Cloud Stores
Enterprise Apps
Databases
Mainframe Data
Splunk Natural Language Processing

Query

Communicate

Automate
- Natural language query
- Text or Voice input
- SPL or SQL
- Disambiguation and Context Correction
- Provide recommendations
- Learn from your actions
- Smart data discovery
What Questions Can I Ask?

- **Time-bound**
  - “sales quarter over quarter in 2015”
  - “sales by country in 2014”

- **Time & Context**
  - “average price Widget X is sold”

- **Aggregation**
  - “products with high sugar content”

- **Identification**
  - “number of service tickets in Q1 vs Q2”
  - “country with highest sales”

- **Comparison**
  - “sales by product excluding Widget X”

- **Ranked**
  - “countries where sales are > 10m”

- **Exclusion**
  - “sum of units sold in Canada by store”

- **Range**

- **Compute**

*conf2017*
Communicate

- Generate relevant visualization
- Interaction via visualization
- Generate narrative - natural language text
- Highlight things of importance
Automate

- Set up alerts
- Set up actions
- Send email or other workflow tasks (example: when voice access returns multiple results, ask to send email)
Demo!
What You Saw

- Natural language queries
- Disambiguation
- Instant results
- Interactive Discovery
- View SPL
- Run in Splunk
Can It Work With Your Data?

Yes!

- Any data model in Splunk
- Or Relational Database
- Or an Enterprise application...
How To Splunk Your Data With Natural Language Queries

1. Connect Data Source
2. Enrich Ontology
3. Parse and Execute Query
4. Communicate results
More Demo!
What You Saw

- Adding your own data source
- Query on non-Splunk data
- Slack client using REST API
Benefits

- Broader appeal
  - Anyone can use
  - Self discovery drives higher engagement
- Faster time to value at lower cost
  - Simplified user experience
  - Productive in seconds
  - Minimal training
- Data driven decisions
  - Analyze structured and unstructured data
  - Historical, Transactional, Operational Data
  - Understand the Why? Not just What?
less like this ...

and more like this ...

come to Papa
See Data Fabric and NLP in Splunk Labs

Sign up for the Beta

dipock@splunk.com

Thank you
Making machine data accessible, usable and valuable to everyone.
Thank You

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