Ask Splunk! Using natural language, voice and chat with Project Natural Language Search

October 2018 | Version 1.0

Our Speakers

DIPOCK DAS

Senior Director,
Products, Splunk

DAYANAND POCHUGARI

Senior Manager,
Engineering, Splunk

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.

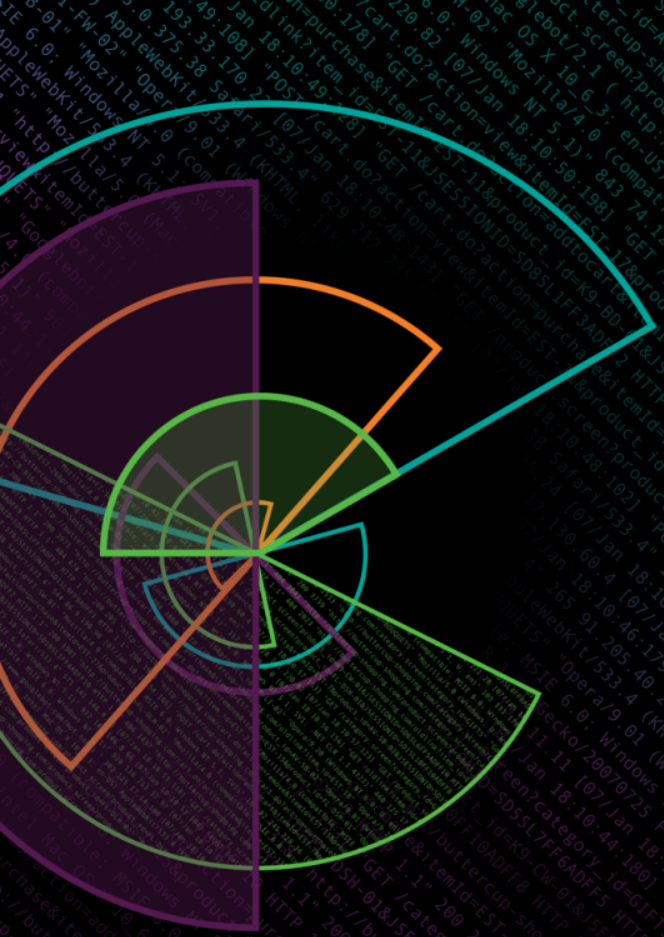
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements 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.

What we will show you ...

1. What is Project Natural Language Search
2. Why it will make your life easier
3. How you can use it

Save your questions

Let’s talk. Visit our booth on the conf floor.



Introduction

Is this you?

Hey, how many security incidents in the last hour ?

Where's that IT report?

Can you update that dashboard to include sales across stores?

Hey what's the SPL for ...

splunk> .conf18

But what about everyone else?

Management

Sales

Marketing

Finance

Shop Floor

Warehouse

Maintenance

Service

Users need the right tools to suit their skills

SPL

Natural Language

What is Natural Language?

How many security incidents in the last hour ?

What were sales quarter over quarter in 2017?

When will we run out of stock?

What is Project Natural Language Search?

Project Natural Language Search is a natural language platform for machine data that delivers Natural Language Search, Understanding and Generation for Splunk and SQL data.

Natural Language Search

Communicate instantly in charts, text and voice

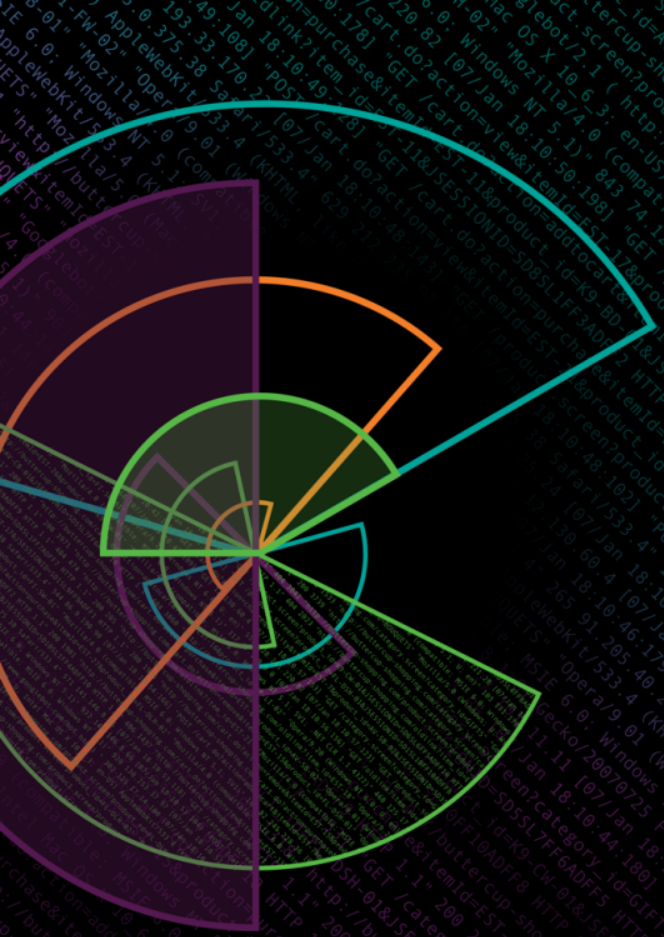
Access anywhere with type, touch, voice

NLS understands the intent then creates the SPL

show	me	daily	sales	of	cappuccino	in	Vancouver	last	10	days
verb	pronoun	adjective	plural	preposition	singular noun	preposition	singular noun		value	plural
predicate		clause	subject		subject		clause			clause
		time grain	sales data		product data		cities			time range from now

Intent: {sum} {sales} {product} {timegrain} {city} {time range}

SPL | tstats allow_old_summaries=t summariesonly=t SUM("All_Sales.grossSales") AS "All_Sales.grossSales" FROM datamodel=Retail.All_Sales WHERE ((("All_Sales.productName"="cappuccino") AND ("All_Sales.city" IN ("vancouver","san francisco","san jose"))) AND ((earliest=1533427200) AND(latest=1534291199))) BY "All_Sales.city" _time span=1d | eval All_Sales__time_date=strftime(_time, "%Y-%m-%d") | table All_Sales__time_date "All_Sales.city" "All_Sales.grossSales"



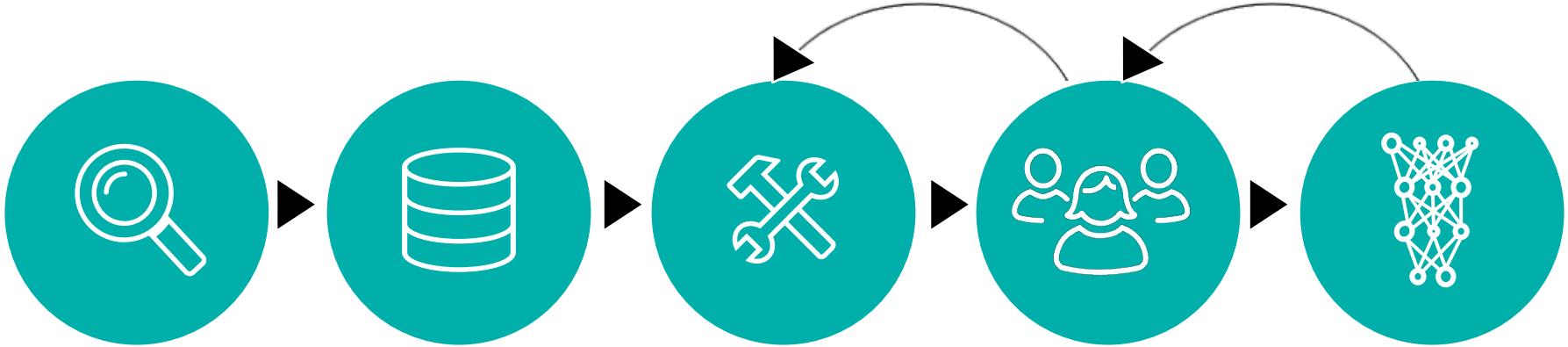
Demo

Can I use it?

1. Yes !!
2. SaaS for On Premise and Cloud customers
3. Needs a Splunk data model - you can create models to suit the questions people want answers to

Model Driven Natural Language Understanding

From raw data to insights - simple steps to NLQ



What questions?

Create a Data model

Enrich Semantic Model

Users ask questions

Trained Machine Learning Model

Creating the Semantic Model

Datamodel

- Entities
- Attributes

Ontology

Administrator

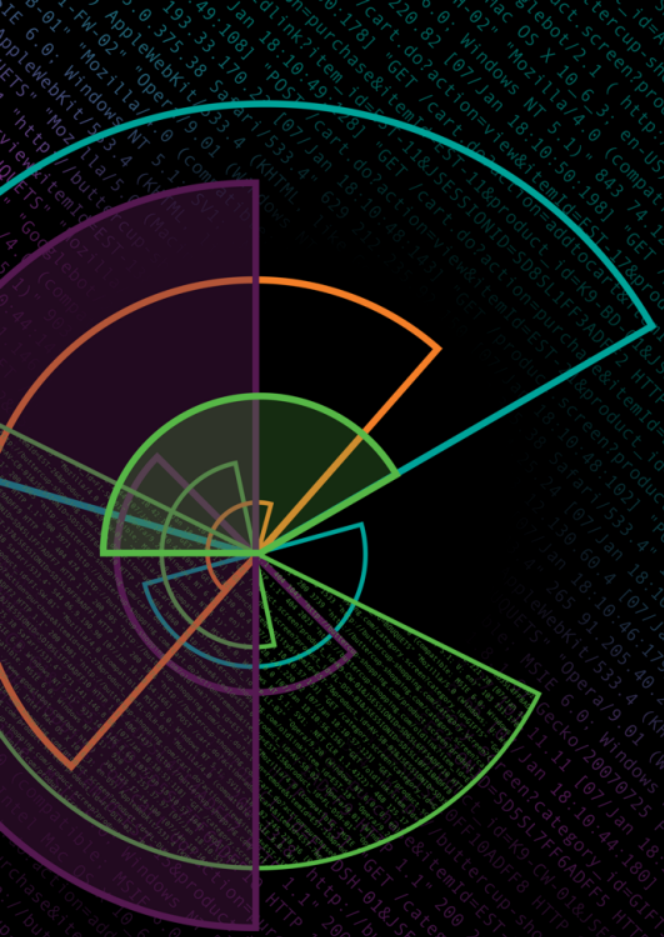
- Named Entities
- Relationships
- Synonyms
- Context

What questions can I ask?

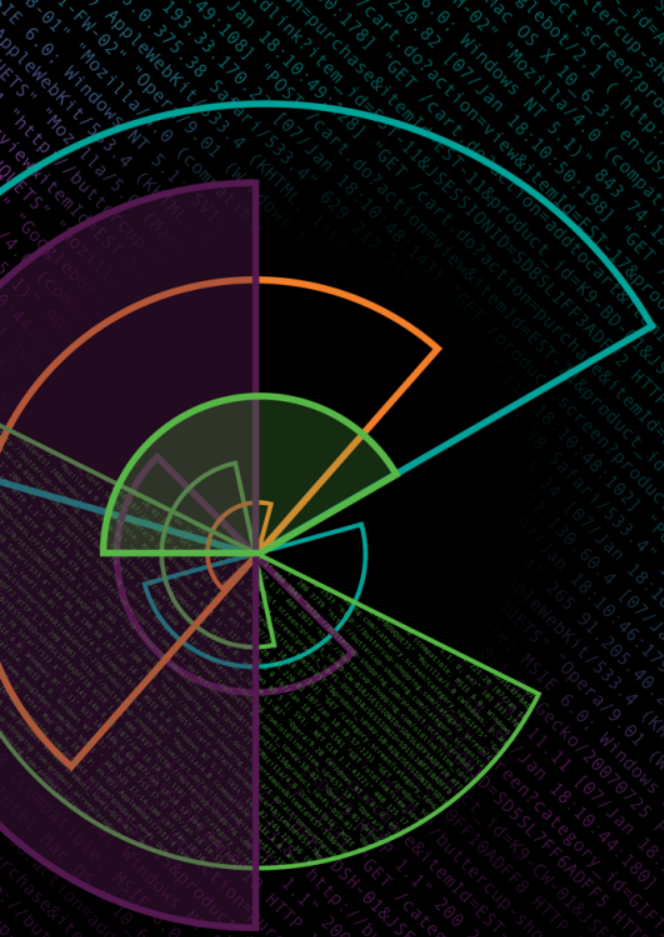
- Time-bound
  - sales quarter over quarter in 2018
  - incidents between 1AM and 2AM by the minute
- Time & Context
  - traffic by country last 5 minutes
  - unusual traffic by IP address
- Compute
  - average sales revenue by City for Widget X
  - what is the standard deviation of sales of X
- Identification
  - show me products with high sugar content
- Comparison
  - number of open service tickets by employee
- Ranked
  - city with the highest sales last week
  - user with the most login failures today

What SPL is supported?

- eval
- stats
- tstats
- group by
- table
- search
- dedup
- where
- Summaries -> allow_old_summaries, summariesonly
- sort with ASC & DESC
- rename
- earliest
- latest
- join
- values
- mvexpand
- span
- predict (with timechart)
- predict using LLP5
- inputlookup
- tail
- output
- not
- in
- rest
- AND & OR
- <,>,= & !=
- LIKE - wildcards (*string*)
- iplocation
- strftime with different formats %b %Y %m..etc
- AVG,SUM,COUNT,STDEV , MIN, MAX

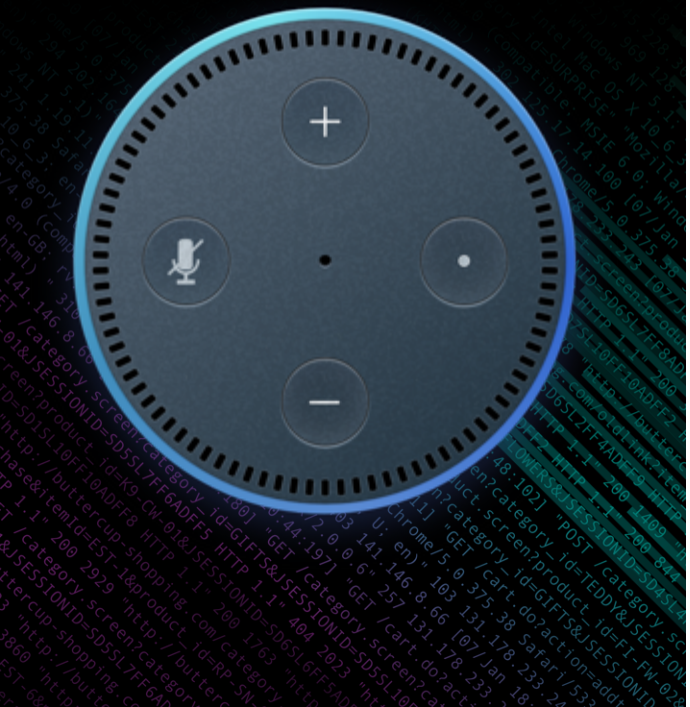


Demo



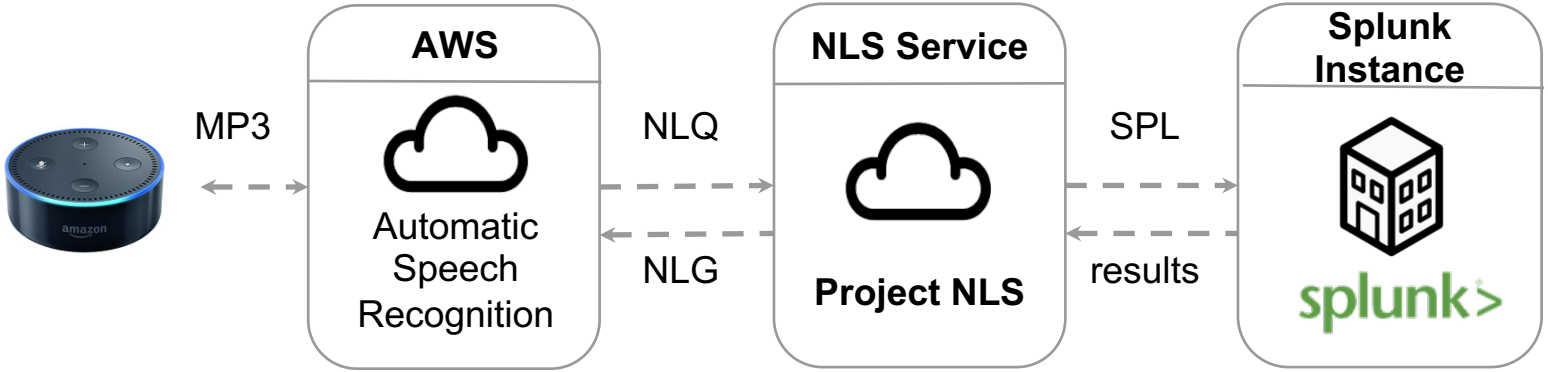
Ask Splunk!

Alexa for Work



- Announced at AWS re:Invent 2017
- What you can do today
  - Ask questions just as you would using the NLS Splunk app
  - Use it for Public data use cases
  - No need to create skills for each use case!!
- How you set it up
  - Connects your Alexa for Work account to a Splunk named user
  - Requires OAUTH
- What it cannot do
  - Does not authenticate user on a per user request

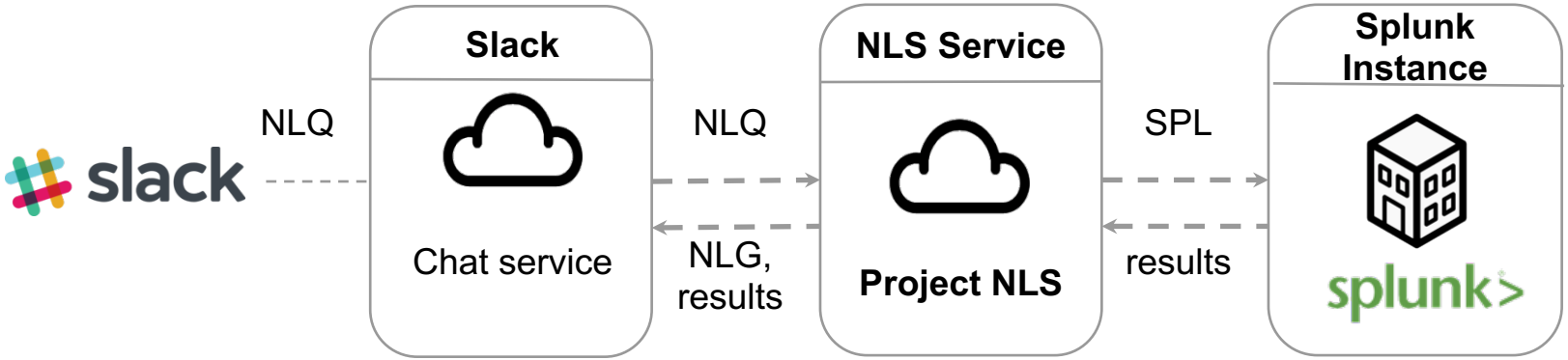
Ask questions using Voice enabled devices



Ask questions using a Chatbot

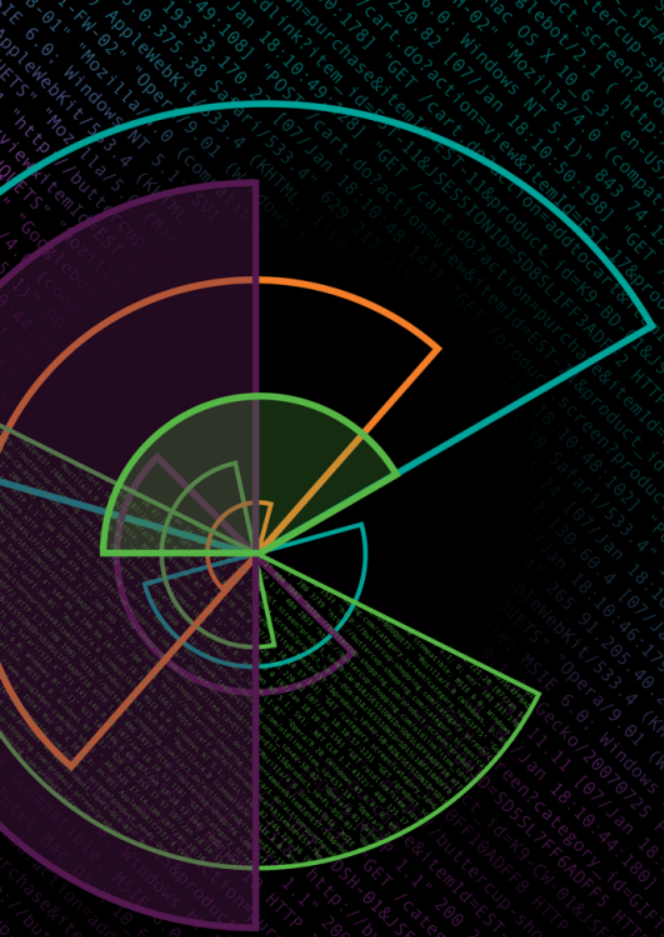
- Slack
- Cisco Webex for Teams
- Custom

Chat enabled



With the NLS REST API - you can be a Superhero !

- Integrate NL into your own apps
- Example: CLI tool
- Get the code: https://github.com/dipoc kdas/jubilee-cli



Demo

Out of the box ontologies for Premium Solutions

Splunk Enterprise Security™

- top 10 malware by host
- show me account lockouts this week
- which servers are listening on ports 80 and 443?
- show users with more than 10 failed logins this week
- show network traffic today by second between 1AM and 3AM
- how many critical vulnerabilities were found today by host and signature?

Splunk IT Service Intelligence™

- Show me all the critical services
- Worst KPIs in Service X
- Worst Entities in KPI X
- Tell me which services will be critical in 30 minutes
- How many tickets are linked to open events
- How many episodes have we closed in the past X hours

We can't guarantee that you can answer all your questions out of the box - but using the ontology workbench you can quickly tailor the semantic model to meet your needs.

Where next?

1. Dialogue/chat based - conversational discovery

2. Behavioral Analytics

3. You decide. Get involved.
   Dipock Das - dipock@splunk.com
   Melissa Gannes - mgannes@splunk.com

Key Takeaways

1. NLS SaaS LAR available for On Prem and Cloud customers
2. Use NLS for your own use cases
3. You can access NLS anywhere

Other sessions

Machine Learning & Natural Language Processing at BMW (FN1199)	**11:30 yesterday**
Spreading the Word: How Chat and Voice Is Transforming Splunk in Retail AI Ops (FN1572)	**4:30 yesterday**
How we use machine learning in Project Natural Language Search - a Natural Language Platform (FN1629)	**11:00 today**

Oh and one last thing …..

Where's that sales report?

top 5 countries by sales last week

daily quantity of spicy chai last week

daily sales in San Francisco last 5 days

sales by minute in San Francisco last 24 hours

splunk> .conf18

Thank You

Don't forget to rate this session in the .conf18 mobile app