Send your spreadsheets to Splunk!

Ryan O'Connor | Senior Advisory Engineer
Satoshi Kawasaki | Splunk for Good Ninja

splunk> .conf19

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, 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. © 2019 Splunk Inc. All rights reserved.

Bio: Ryan O'Connor

MS in Business Analytics and Project Management

1) **Joined Splunk in 2018**

   Splunk User for 8+ Years

   Joined Splunk Trust in 2017

   Joined Splunk in 2018 - Emerging Products Advisory Team

   Wrote apps for Nest, HealthKit, and many more...

2) **Previous conf talks:**

   conf17: *Taking Splunk Inside the Classroom*

3) **This year's conf talks:**

   conf19: *Monitoring Aquaponics Facilities Around the Globe*

   conf19: *Send your spreadsheets to Splunk!*

Bio: Satoshi Kawasaki

BS in Aerospace Engineering from Georgia Tech

hobbes3

1) **Joined Splunk in 2013**

   3 years in Splunk Professional Services (PS)

   3+ years in Splunk for Good

2) **Previous conf talks:**

   conf14: *I want that cool viz in Splunk!*

   conf15: *Enhancing dashboards with javascript!*

   conf17: *Speed up your searches!*

   conf17: *Splunking to fight human trafficking!*

   conf17: *Splunking the 2016 presidential election!*

3) **This year's conf talks:** YOU ARE HERE

   conf19: *Speed up your searches!*

   conf19: *Splunking refugees with help from NetHope and Cisco!*

   conf19: *Splunking the 2018 midterm election!*

   conf19: *Send your spreadsheets to Splunk!*

splunk> .conf19

Splunk for Good

Big data can make a big difference

- $100 million Splunk Pledge has issued licenses and training worth over $40 million.
- Workforce training initiatives for veterans, students and opportunity youth have reached more than 10,000 people.
- Engaging our partners in initiatives to promote STEM and develop shared solutions for humanitarian response and human trafficking.
- Supporting life-changing research at top universities.
- More than 100,000 hours of paid volunteer time.

WOUNDED WARRIOR PROJECT®

NETHOPE

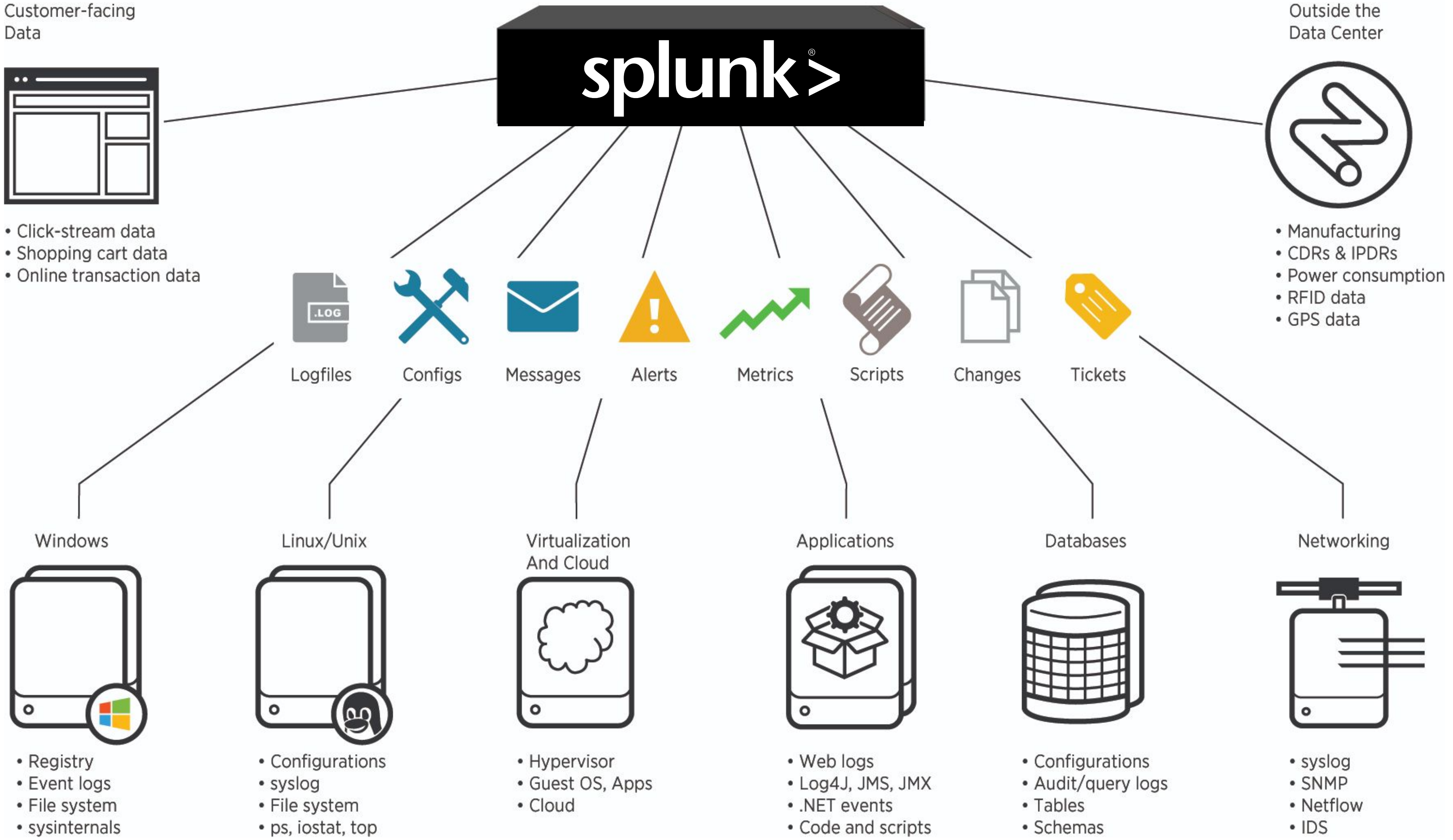
TEAM RUBICON

npower

Table of Contents

1) Intro
2) Why spreadsheets?
3) Splunk App for Google Sheets
4) Installation and configuration
5) Usage
6) Best practices
7) Next steps

Intro: What Splunk can index



Customer-facing Data

- Click-stream data
- Shopping cart data
- Online transaction data

Outside the Data Center

- Manufacturing
- CDRs & IPDRs
- Power consumption
- RFID data
- GPS data

Windows

- Registry
- Event logs
- File system
- sysinternals

Linux/Unix

- Configurations
- syslog
- File system
- ps, iostat, top

Virtualization And Cloud

- Hypervisor
- Guest OS, Apps
- Cloud

Applications

- Web logs
- Log4J, JMS, JMX
- .NET events
- Code and scripts

Databases

- Configurations
- Audit/query logs
- Tables
- Schemas

Networking

- syslog
- SNMP
- Netflow
- IDS

BUT spreadsheets!

Pros and cons

- Everyone understands them (easy to use).
- It's not strict (like databases).
- You can use them to create formulas, charts, and dashboards.
- Easy to share!
- So many free software!

- They are entered by humans.
- Need to saved/converted to CSV.
- You thought SPL was hard to write and troubleshoot?
- You can use them to create formulas, charts, and dashboards.

Google Sheets

Many organizations, especially small ones, still rely on spreadsheets

Part of **Google Drive** suite of tools.

Free to individuals and nonprofits (Google for Nonprofits).

Designed with collaboration in mind with link sharing, permission system, automatic version controls, and commenting.

Splunk App for Google Sheets

Available today!

Open Source and available on Github:

- https://github.com/ryanwoconnor/GoogleDriveAddonforSplunk

Distributed on Github due to the reliance on two Python packages.

- BeautifulSoup[1]
- Pandas[1]

Setup time is less than 2 minutes.

[1]BeautifulSoup and Pandas are not distributed with Splunk today

Splunk App for Google Sheets

Written in Python

Comes with several SPL Commands[1]:

- `getcsv` - list csv files in your drive.
- `getchanges` - list any changes in your Drive.
- `exportcsv` - stream a specific csv to splunk.
- `exportsheethtml` - stream a specific sheet to splunk (with merged cell support).
- `exportsubsheet` - export a specific subsheet.
- `subsheetlist` - list subsheets in a sheet.
- `deletegooglekey` - delete your Google API Key from Splunk.

[1] You can create commands like this too! http://dev.splunk.com/view/python-sdk/SP-CAAAEU2

Bonus! Google Classroom

Why not manage your gradebook in Splunk?

Also in this app are a few commands to stream in Google Classroom data.

- **`listcourseworksubmission`** **-** list submissions for coursework.
- **`liststudents`** **-** list students in your course.
- **`listcoursework`** - list assigned coursework.
- **`listcourse`** - list your courses.

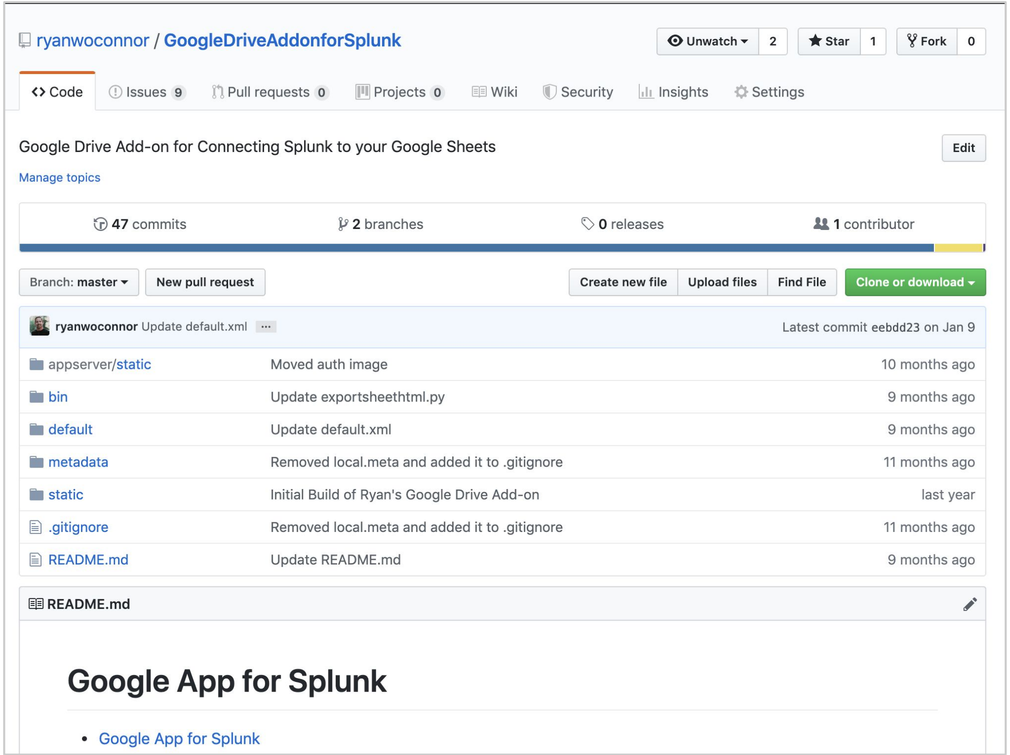
Installation Guide

Full installation Guide is included on Github.

- Includes a YouTube video!

High Level Steps:

- Install Google App for Splunk.
- Install Python for Scientific Computing.
- Configure apps.
  - Setup Google App for Splunk.
  - Setup Google App with custom python libraries.



Google Drive Add-on for Connecting Splunk to your Google Sheets

ryanwoconnor Update default.xml … Latest commit eebdd23 on Jan 9

appserver/static	Moved auth image	10 months ago
bin	Update exportsheethtml.py	9 months ago
default	Update default.xml	9 months ago
metadata	Removed local.meta and added it to .gitignore	11 months ago
static	Initial Build of Ryan's Google Drive Add-on	last year
.gitignore	Removed local.meta and added it to .gitignore	11 months ago
README.md	Update README.md	9 months ago

README.md

Google App for Splunk

- Google App for Splunk

Best Practices

Keep the spreadsheet **machine-friendly**, not human-friendly.

- The app doesn't care about charts, legends, info box, colored/formatted cells, etc.
- Keep the spreadsheet simple and consistent.
- Create charts and do all that fancy stuff in Splunk instead!

First row of your sheet should always be a header (ie column names).

Don't have empty rows.

Don't merge cells.

- The app supports merged cells (with Pandas and BeautifulSoup), but it's still not recommended.

Don't use long or human-friendly column names.

- Use something like "sec_0_to_60" over "Seconds to get from 0 and 60 mph".

Using the App

Choose Your Own Adventure

If you've followed Best Practices, you're going to have a good time.

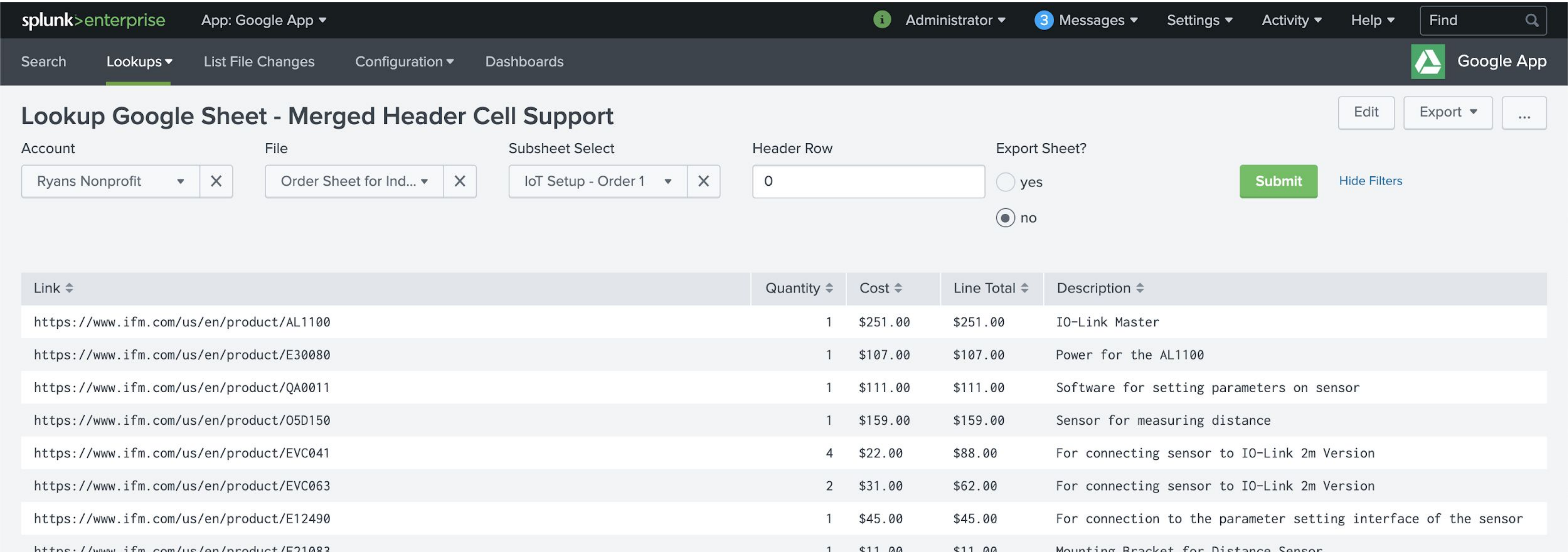
We've provided a nice set of dashboards for getting started.

- Lookup Google Sheet.
  - The original dashboard.
- Lookup Google Sheet - Merged Header Cell Support.
  - This dashboard is one we added for merged cell support.
- List File Changes.
  - Dashboard to list file changes in your Google Drive (useful for alerting on file changes).

Using the App

Utilizing Built-in Dashboards

Easiest way to start to analyze data from your sheets is to use the dashboards.



Lookup Google Sheet - Merged Header Cell Support

Account: Ryans Nonprofit

File: Order Sheet for Ind...

Subsheet Select: IoT Setup - Order 1

Header Row: 0

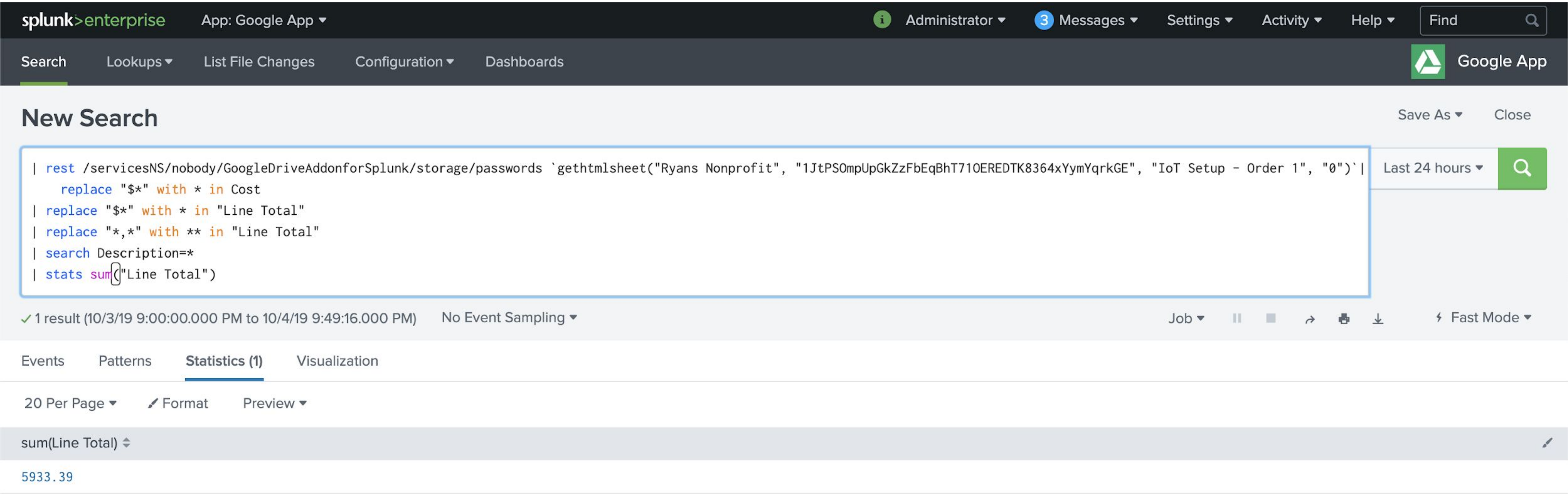
Export Sheet?
○ yes
● no

Link	Quantity	Cost	Line Total	Description
https://www.ifm.com/us/en/product/AL1100	1	$251.00	$251.00	IO-Link Master
https://www.ifm.com/us/en/product/E30080	1	$107.00	$107.00	Power for the AL1100
https://www.ifm.com/us/en/product/QA0011	1	$111.00	$111.00	Software for setting parameters on sensor
https://www.ifm.com/us/en/product/O5D150	1	$159.00	$159.00	Sensor for measuring distance
https://www.ifm.com/us/en/product/EVC041	4	$22.00	$88.00	For connecting sensor to IO-Link 2m Version
https://www.ifm.com/us/en/product/EVC063	2	$31.00	$62.00	For connecting sensor to IO-Link 2m Version
https://www.ifm.com/us/en/product/E12490	1	$45.00	$45.00	For connection to the parameter setting interface of the sensor
https://www.ifm.com/us/en/product/E21083	1	$11.00	$11.00	Mounting Bracket for Distance Sensor

Using the App

Creating a Search

Our app streams your data into Splunk results. Then unleash your SPL-fu!



New Search

```
| rest /servicesNS/nobody/GoogleDriveAddonforSplunk/storage/passwords `gethtmlsheet("Ryans Nonprofit", "1JtPSOmpUpGkZzFbEqBhT71OEREDTK8364xYmYqrkGE", "IoT Setup - Order 1", "0")`|
    replace "$*" with * in Cost
| replace "$*" with * in "Line Total"
| replace "*,*" with ** in "Line Total"
| search Description=*
| stats sum("Line Total")
```

✓ 1 result (10/3/19 9:00:00.000 PM to 10/4/19 9:49:16.000 PM) No Event Sampling ▾

sum(Line Total)
5933.39

Going Forward

The future

We’d like to keep developing this app!

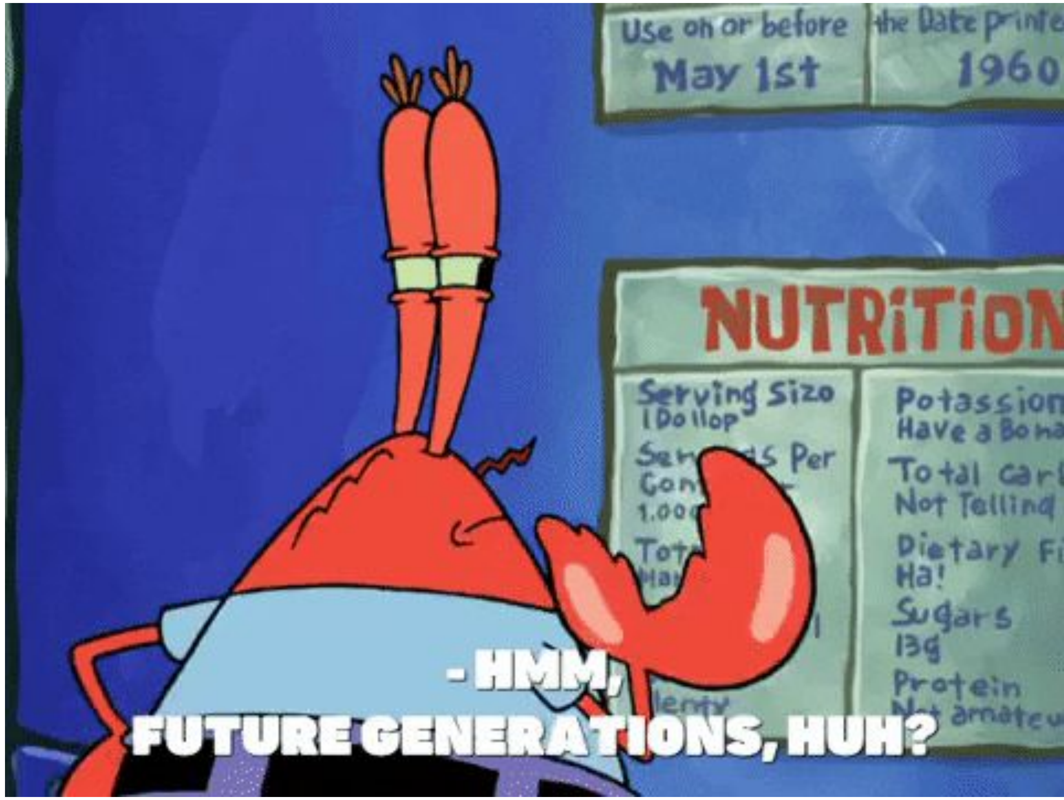
Haven’t handled every edge case

Spreadsheets have some features and tools that allow it to work as:

- A database
- A data visualization platform
- A data science tool

So we need your feedback!

- (And we’d love to collaborate)



Q&A

Ryan O'Connor | Senior Advisory Engineer
Satoshi Kawasaki | Splunk for Good Ninja

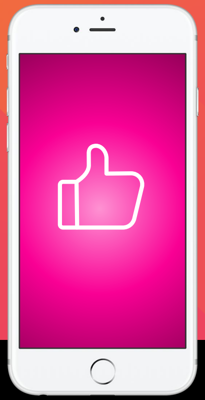
.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

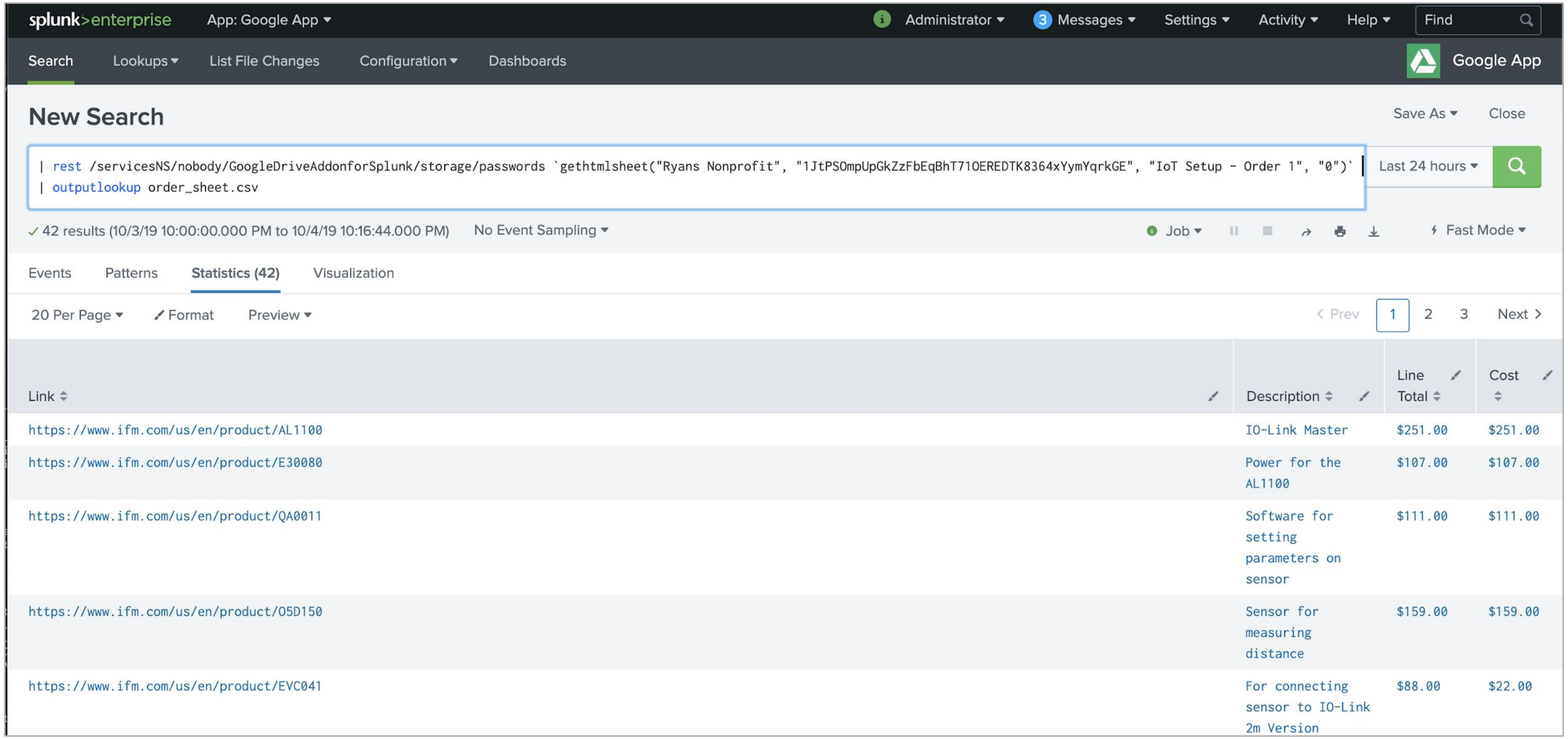
RATE THIS SESSION



Using the App

Don't forget you can even save the result

Don't forget you can even save the result



New Search

```
| rest /servicesNS/nobody/GoogleDriveAddonforSplunk/storage/passwords `gethtmlsheet("Ryans Nonprofit", "1JtPSOmpUpGkZzFbEqBhT71OEREDTK8364xYymYqrkGE", "IoT Setup - Order 1", "0")`
| outputlookup order_sheet.csv
```

✓ 42 results (10/3/19 10:00:00.000 PM to 10/4/19 10:16:44.000 PM) No Event Sampling ▾

Link	Description	Line Total	Cost
https://www.ifm.com/us/en/product/AL1100	IO-Link Master	$251.00	$251.00
https://www.ifm.com/us/en/product/E30080	Power for the AL1100	$107.00	$107.00
https://www.ifm.com/us/en/product/QA0011	Software for setting parameters on sensor	$111.00	$111.00
https://www.ifm.com/us/en/product/O5D150	Sensor for measuring distance	$159.00	$159.00
https://www.ifm.com/us/en/product/EVC041	For connecting sensor to IO-Link 2m Version	$88.00	$22.00