

# 40 9 Must-Have Apps and Why You Are Crazy Nøt to Use Them!

Presented by Splunxter father & son team:

Gregg Woodcock - Senior Splunk Architect

Woodcock@Splunxter.com

Noah Woodcock - Certified Splunk Admin Noah@Splunxter.com

October 2018 | Version 1.0

#### 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. © 2018 Splunk Inc. All rights reserved.



#### Meet Your Co-Presenters

We are not the only father-and-son team @ Splunxter; Mark & Dave Allen are here, too!

#### **Gregg Woodcock**

- Splunking full-time since 2009
  - Splunk Certified Everything Splunk Trustee
    - Currently #4 on answers.splunk.com
      - Exaggerated w/ BS since 17 years old!

Working on Private Pilot License since 1984

Career Highlight: Starting my own Splunk-focused consulting company and getting to work with my family



- Splunking full-time since 2015
  - Splunk Certified Admin & SEIII
    - Currently #2628 on answers.splunk.com
      - Graduated w/ BS from Texas A&M at 17 years old!

Working on Private Pilot License since 2017

Career Highlight: ArcSight rip-and-replace and custom SIEM for huge multinational



#### We cannot cover every great app

So we cover the stuff that is most important to us and our clients



#### **Data Integrity:**

Data Curator

Meta Woot!

Alerts for Splunk Admins



#### **Config Management:**

Lookup Editor
Gemini KV Store Tools
Configurations Analytics



#### **Dashboard Development:**

Dashboard Examples
Developer Gadgets
Infobutton



"Whatsoever things are true, whatsoever things are honest, whatsoever things are just, whatsoever things are pure, whatsoever things are lovely, whatsoever things are of good report; if there be any virtue, and if there be any praise, think on these things."

Splunk translation: Garbage In, Garbage Out.

Have you ever take a good look at the core quality of your event data? Apps can help.

1: Data Curator

- 1. Focus on the "dm\_date\_parsing\_issues" screen; eliminate all errors.
- 2. Generally the solution is to tell Splunk exactly where/what the **timestamp** is.
- 3. Evaluate these key **props.conf** timestamp settings in the dirlldowns:
  - \* LINE BREAKER
  - \* MAX TIMESTAMP LOOKAHEAD
  - \* SHOULD\_LINEMERGE
  - \* TIME FORMAT
  - \* TIME PREFIX
  - \* TRUNCATE
  - \* **TZ**





2: Meta Woot!

- Focus on the main "meta\_woot\_search" screen; eliminate all the red.
- 2. Generally the solution is to tell Splunk exactly what TZ should be applied.
- 3. Remember that a "TZ=" in props.conf on the UF has the highest precedence so consider using a set of TZ-specific props.conf apps with appropriate whitelist on your Deployment Server. Also, "TZ\_ALIAS=" can be used to override an incorrect TZ value inside events!



3: Alerts for Splunk Admins

- Provides almost 100 alerts and dashboards but requires configuring and upkeep of macros that describe your topology (Search Heads, Indexers, etc.)
- 2. Splunk is good about logging things, but who ever looks at those logs? This app does and it will help you troubleshoot and actionalize!
- 3. Helps you learn and **enforce best- practices** by telling you when users are violating them.



# "Let all things be done decently and in order."

Splunk translation: Have a disaster plan.

For short-term safety, apps can make backups and track configuration changes.



# Key Takeaways 4: Lookup Editor

- 1. Be aware that this app makes a **timestamped backup** every time you click "Save". This can be either a good or a bad thing, depending on your situation and point of view.
- 2. This app is **compatible** for use on a Search Head Cluster (SHC).
- 3. Provides extra features, especially on older versions of splunk (deleting files, moving between apps, import/export, cut-and-paste GUI).



# Key Takeaways 5: Gemini KV Store Tools

- If you are using Search Head Clustering (SHC) and KVStore, be 100% assured that you will eventually have corruption.
- You can schedule backups to a local disk as well as syncs with another Search Head Cluster (push only).
- 3. If you backup to local disk (highly suggested), you should make **periodic** archives from there with **custom** scripts.

### CA

# Key Takeaways 6: Configurations Analytics

- Configuration/Packaging is a bit unusual (3 apps in 1) so READ THE README. Uses hard-coded index values of "conf" and "view".
- 2. Yes, "index=\_audit" shows you who modified a configuration file, but it does not show you what was the change, so how can you roll it back?
- 3. Has dashboard forms that show changes over time.

### "Truly, this only I have found: That God made man upright, But they have sought out many schemes."

Splunk translation: SimpleXML isn't as simple as we would all like it to be.

Apps can show working examples and expose debug in real-time.



7: Dashboard Examples

- Even if you don't need anything now, install it and have a look around. You may find things (e.g. pan and zoom, geo/KML) that you didn't even know SimpleXML could do!
- 2. Drilldown is complicated, especially for beginners; start with a working example from "Drilldown Elements".
- 3. Be sure to check out the last section on "Token Customization". This is a key component to higher-level dashboarding.





8: Developer Gadgets

- Adds token debugger to any dashboard (show/hide it at any time). Never write throw-away debug dashboard panels again!
- 2. You also get "Accordion Panels" javascript. Debugging gets even easier when the only panel you are fixing is at the top and is the only one visible!
- 3. Screen still too busy? Once your inputs are set, hide all of them with a click. Need to refresh your panel? You have a **submit button** that floats stickily in the lower right corner, just click.





- 1. It only does 2 things but both are great for **long-winded instructions** which people only need to see once.
- 2. Adds a clickable "i" icon in the upperright corner of any panel. Click it to get an in-lined area of accordion-text immediately below.
- 3. Adds a clickable "?" icon in the upper-right corner of any panel. Click it to get a popup dialog window in the foreground with an "OK" button to dismiss.



Noah Woodcock | The handsome, clever guy (on right)

Gregg Woodcock | The old^H^H^H experienced guy (on left)

# Thank You

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

.Conf18
splunk>

#### **Bonus Apps**

Some of the other apps that we considered but did not have time/room to cover.

#### "URL Toolbox" app

 Correctly parse URLs and complicated TLDs using the Mozilla Suffix List (to get "domain" field), plus Shannon entropy, counting, suites, meaning ratio, Bayesian analysis, and more!

#### "TA-SyncKVStore" app

 Similar to "Gemini KV Store Tools" w/ encrypted credential storage, Modular Alert to send search results to remote KVStore, and Modular Inputs to pull remote KVStore to local KVStore or index as JSON!

# "GetWatchList" app

 Custom search command for Splunk which will return a CSV formatted list from a URL!

# "Knowledge Object Explorer" app

 Do you need a good reason to delete unused TAs/apps? Not sure why your searches have slowed down so much? This can help explain the hidden tragedy!

# "Data Governance" app

 For a different take on the data quality problem PLUS a view on users/roles and activity/access.

# "Dashboard Assistant" app

 Similar to "Infobutton" but with a different look-and-feel plus versioning capabilities.