© 2017 SPLUNK INC.

splunk> .conf2017

Visualizing the Health of Your Mobile App

Jay Tamboli | iOS Engineer, Capital One

September 26, 2017 | Washington, DC

© 2017 SPLUNK INC.

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.

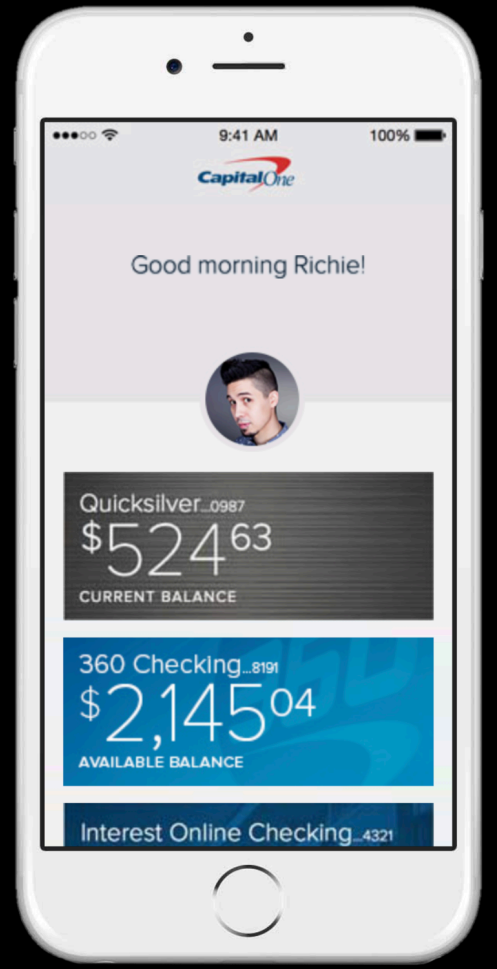
Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

splunk> .conf2017

© 2017 SPLUNK INC.

Capital One for iPhone/iPad

- Check balances, pay bills, deposit checks, redeem rewards, etc.
- Winner, J.D. Power and Associates 2017 U.S. Banking App
- Millions of users

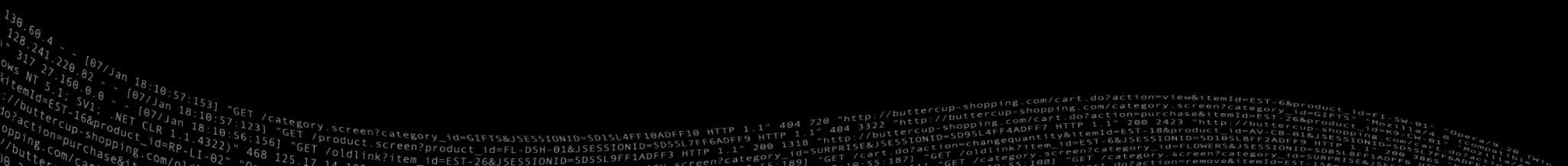


splunk> .conf2017

© 2017 SPLUNK INC.

Agenda

- Why use Splunk instead of client-side analytics?
- Handle large volumes of data by narrowing your scope
- Visualize your results



splunk> .conf2017

© 2017 SPLUNK INC.

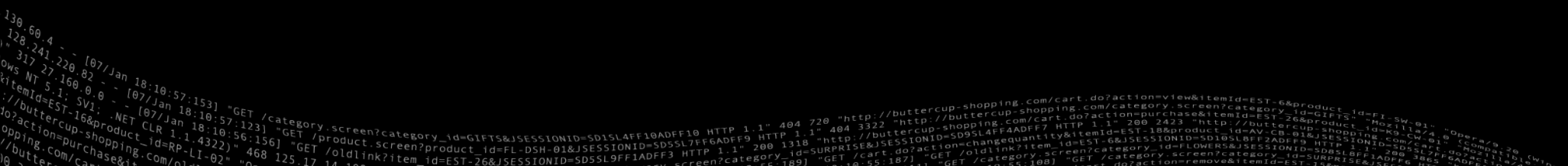
Why not client analytics?

Client analytics

- Might not have instrumentation for all code paths
- Doesn't cover unexpected behavior
- Doesn't include server error

Splunk

- Faster
- Easier comparison across metrics
- Easy, flexible visualizations



splunk> .conf2017

© 2017 SPLUNK INC.

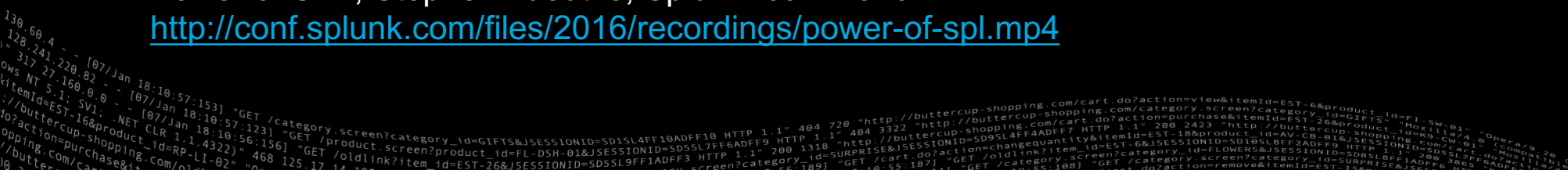
Narrow your events

Limit the scope ASAP

search and filter | munge | report | cleanup

- Everything you do after the search step will benefit from less data to process
- `index=security | spath "response.loginStatus" | search "response.loginStatus"=DENIED`

Power of SPL, Stephen Luedtke, Splunk .conf 2016
http://conf.splunk.com/files/2016/recordings/power-of-spl.mp4



splunk> .conf2017

© 2017 SPLUNK INC.

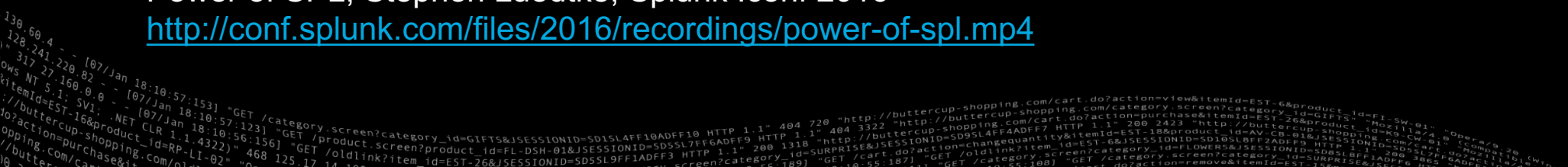
Narrow your events

Limit the scope ASAP

search and filter | munge | report | cleanup

- Everything you do after the search step will benefit from less data to process
- `index=security DENIED | spath "response.loginStatus" | search "response.loginStatus"=DENIED`

Power of SPL, Stephen Luedtke, Splunk .conf 2016
http://conf.splunk.com/files/2016/recordings/power-of-spl.mp4



splunk> .conf2017

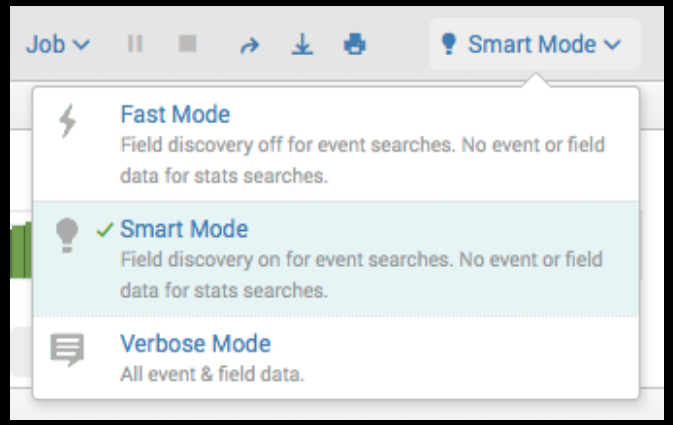
© 2017 SPLUNK INC.

Narrow your events

Limit the scope ASAP

search and filter | munge | report | cleanup

- Everything you do after the search step will benefit from less data to process
- `index=security` **`DENIED`** `| spath "response.loginStatus" | search "response.loginStatus"=DENIED`
- Sampling
- Fast mode
  Or even `| stats count`



Power of SPL, Stephen Luedtke, Splunk .conf 2016
http://conf.splunk.com/files/2016/recordings/power-of-spl.mp4

splunk> .conf2017

© 2017 SPLUNK INC.

Narrow your events

Comparing Thursday to Thursday of the previous week

- ```
  index=access URL="/v1/login" date_wday=thursday
    | timechart count span=1h
    | timewrap w
    | where strftime(_time,"%u")="4"
  ```
- Time range of 1 week means that search head retrieves a lot of data, so limit it to what you really need.

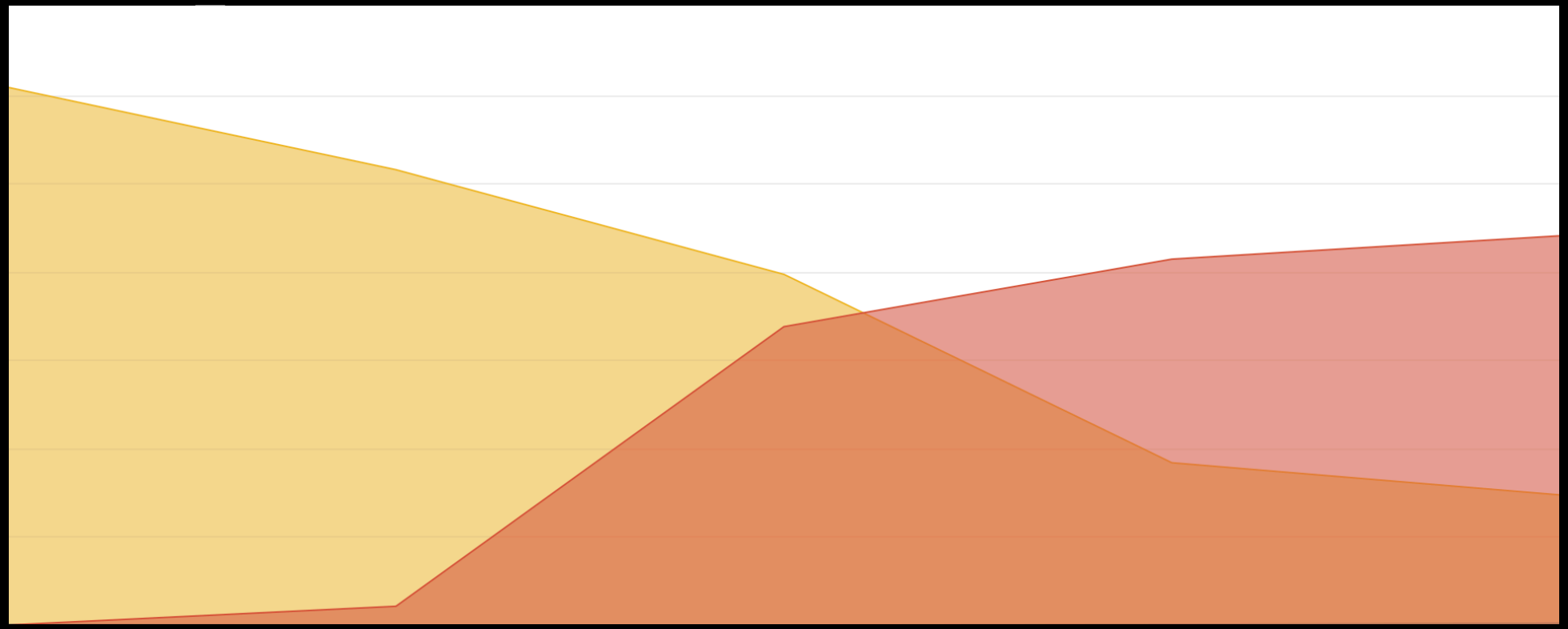
splunk> .conf2017
  ```

© 2017 SPLUNK INC.

Case study: spike in call rate

Visual

- `index=access URL="/v1/login" | timechart count by client_version`



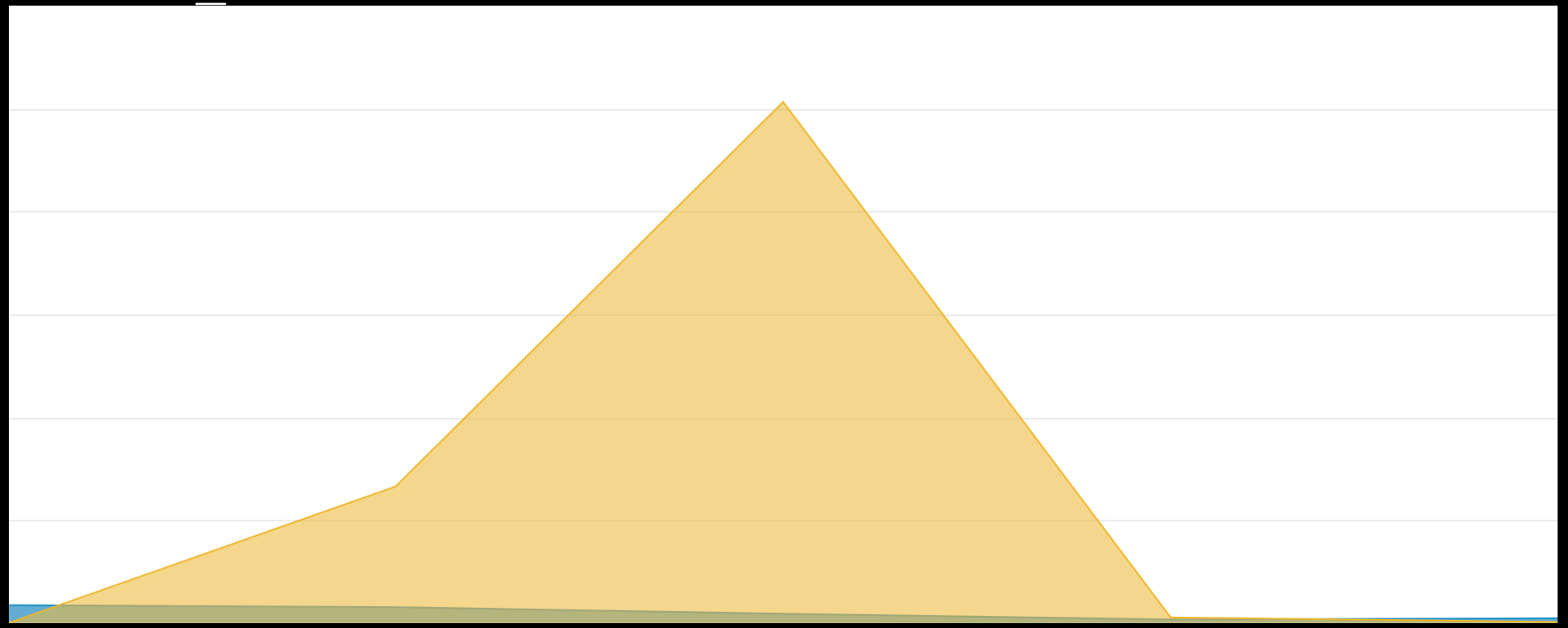
splunk> .conf2017

© 2017 SPLUNK INC.

Case study: spike in call rate

Visual

- `index=access URL="/v1/balances" | timechart count by client_version`



splunk> .conf2017

© 2017 SPLUNK INC.

Case study: spike in call rate

Numbers

```
index=access URL="/v1/login" OR URL="/v1/balances"
| stats count(eval(URL="/v1/login")) as logins_count,
count(eval(URL="/v1/balances")) as balances_count by
client_version
| eval balances_per_session=balances_count/logins_count
```

client_version	logins_count	balances_count	balances_per_session
1.5	4000	3972	0.993
1.6	3500	67234	19.2096864

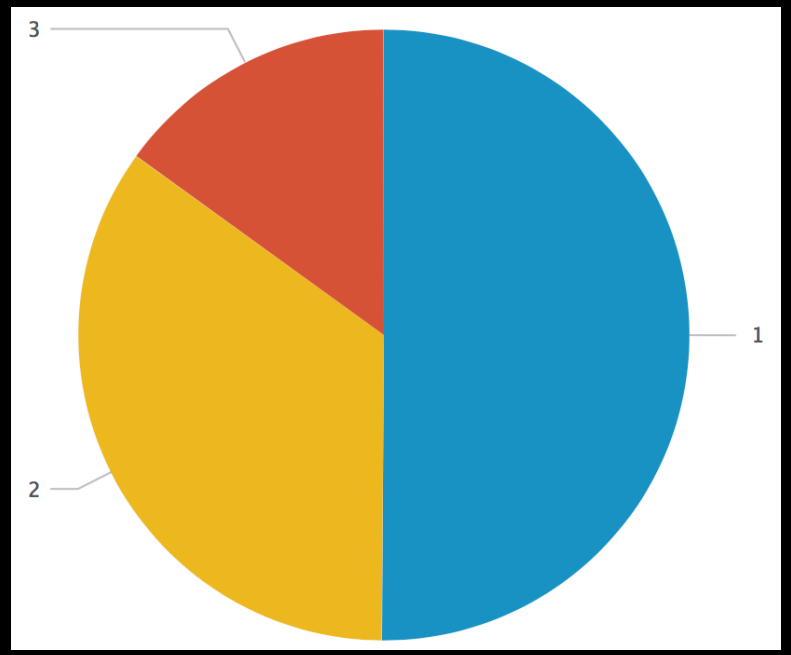
splunk> .conf2017

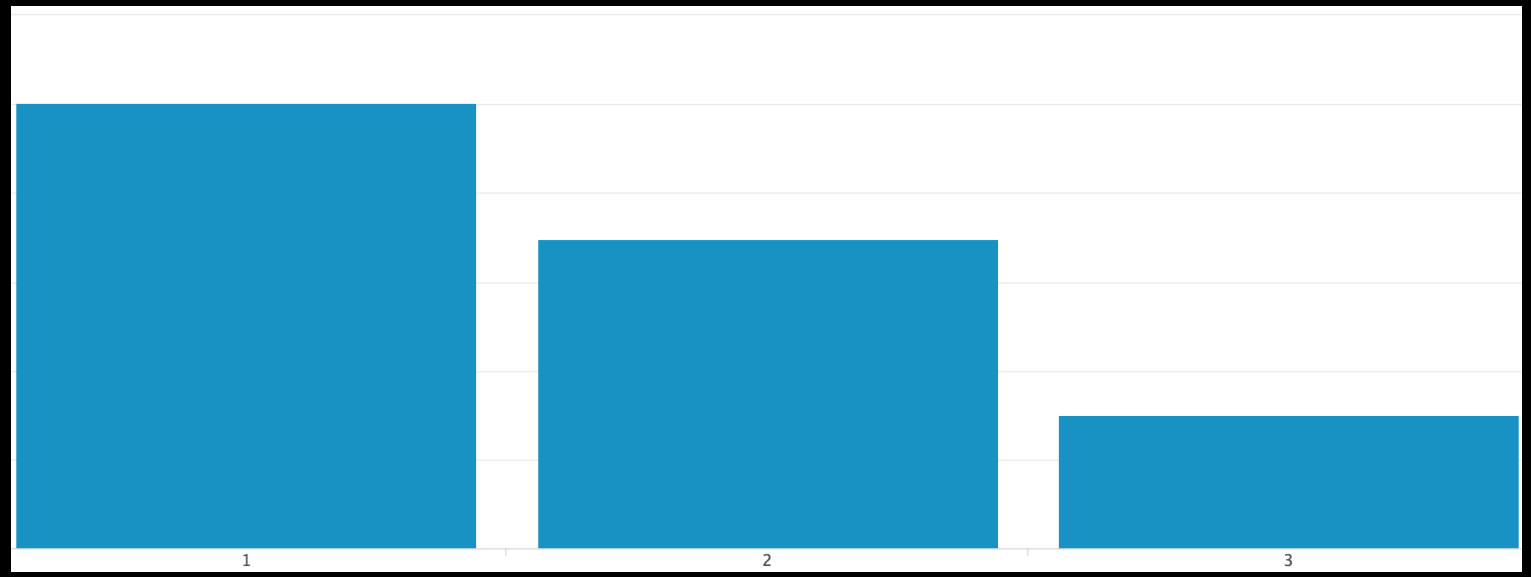
© 2017 SPLUNK INC.

Deciding on a visualization

What is the question you're answering?

- Knowing the question also determines your search
  - App version by launch or by login
- Do you want the fraction of the whole, or how the populations compare?





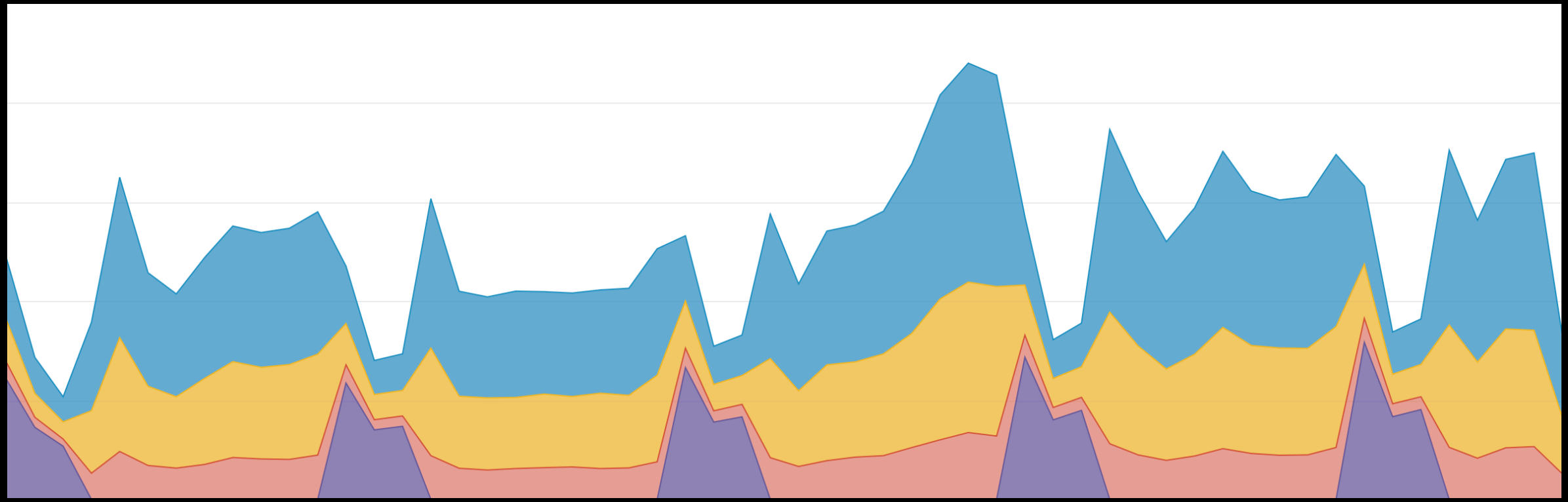
splunk> .conf2017

© 2017 SPLUNK INC.

Deciding on a visualization

Area charts

- Area charts and statistics can hide significant trends in overall volume. Purple is ~10%.



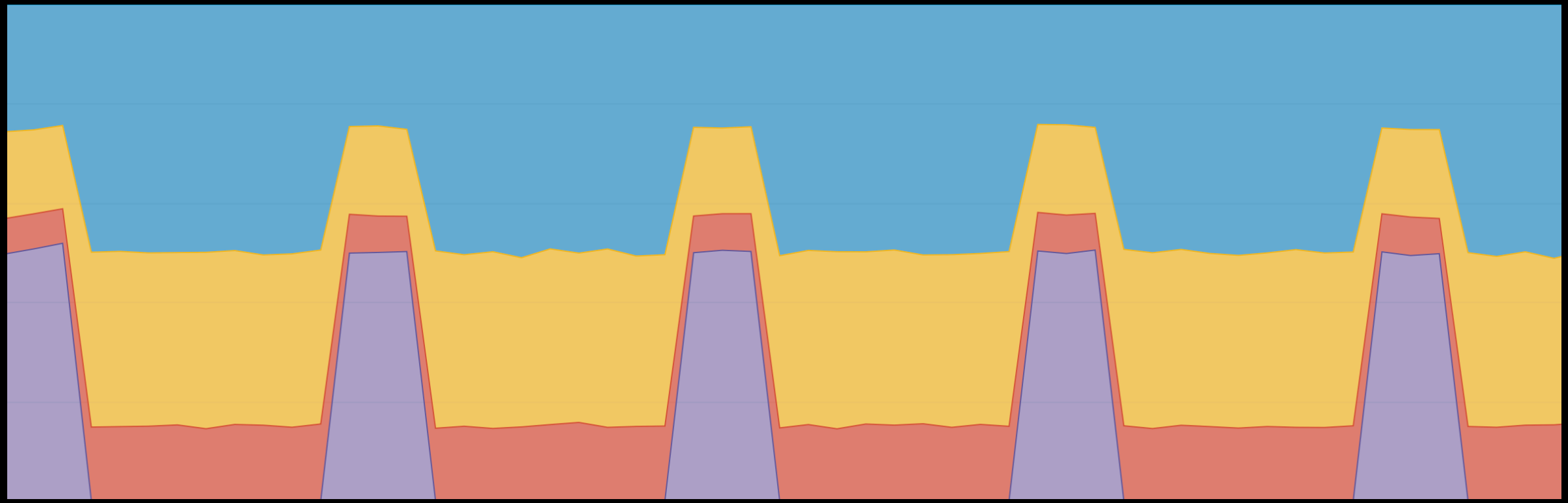
splunk> .conf2017

© 2017 SPLUNK INC.

Deciding on a visualization

Area charts

- Area charts can hide significant trends in overall volume, so use Stacked 100%, and play with your `span(=2h)`. Purple is 50% at late night.



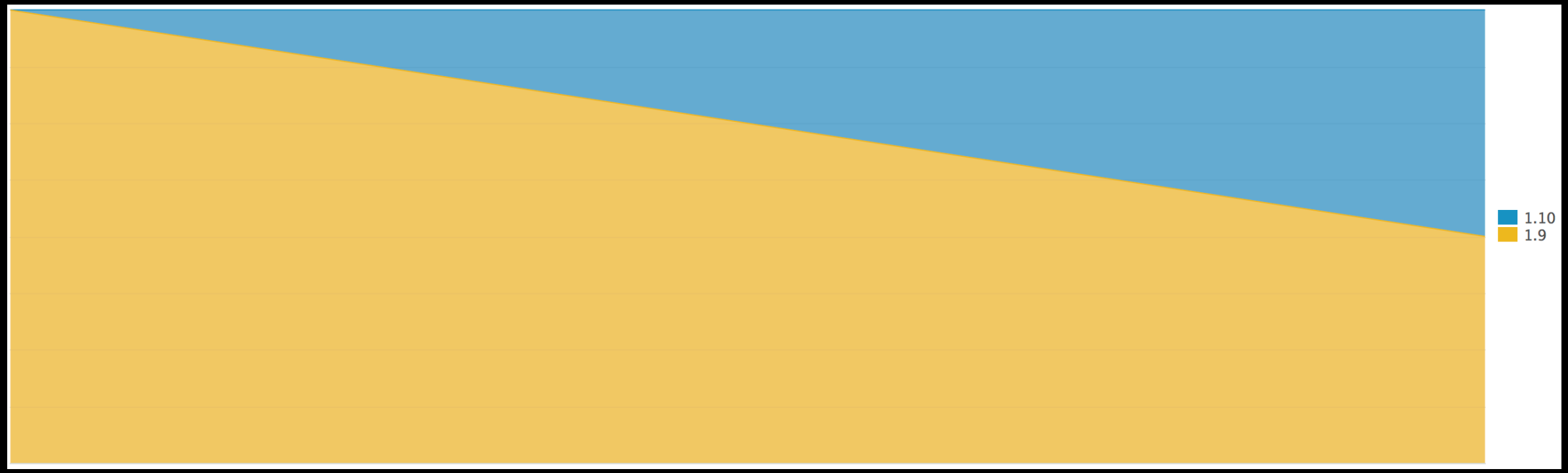
splunk> .conf2017

© 2017 SPLUNK INC.

Ordering groupings in a chart

`timechart` is just a table

- Pipe the output of `timechart` to `| table _time, first, second, etc.`



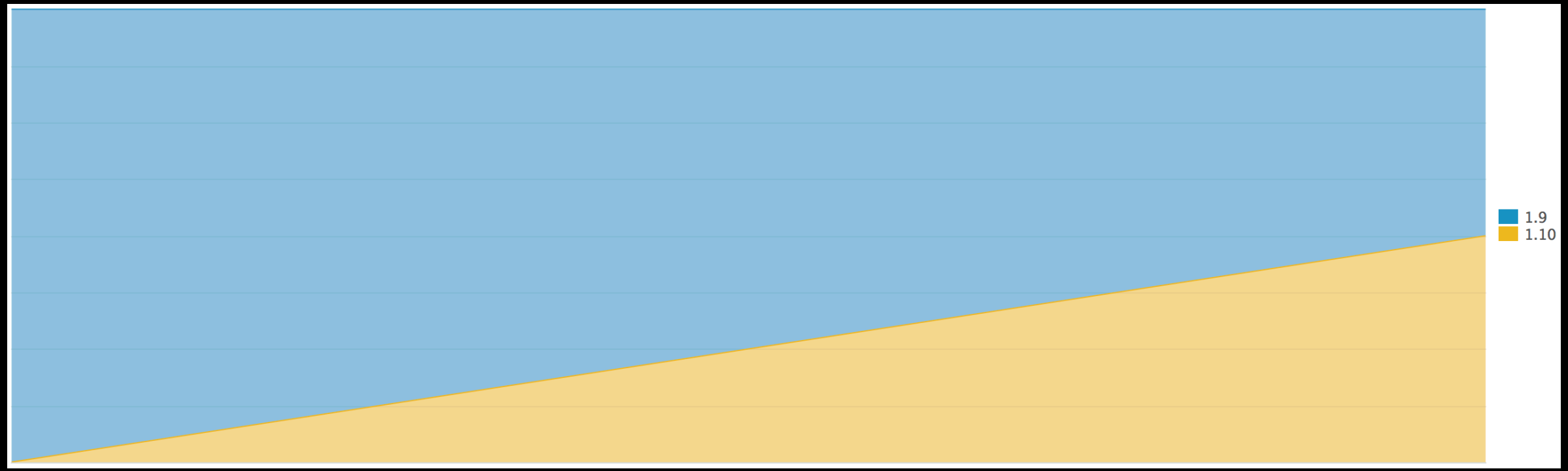
splunk> .conf2017

© 2017 SPLUNK INC.

Ordering groupings in a chart

`timechart` is just a table

- Pipe the output of `timechart` to `| table _time, first, second, etc.`
- `timechart … | table _time, “1.9”, “1.10”`



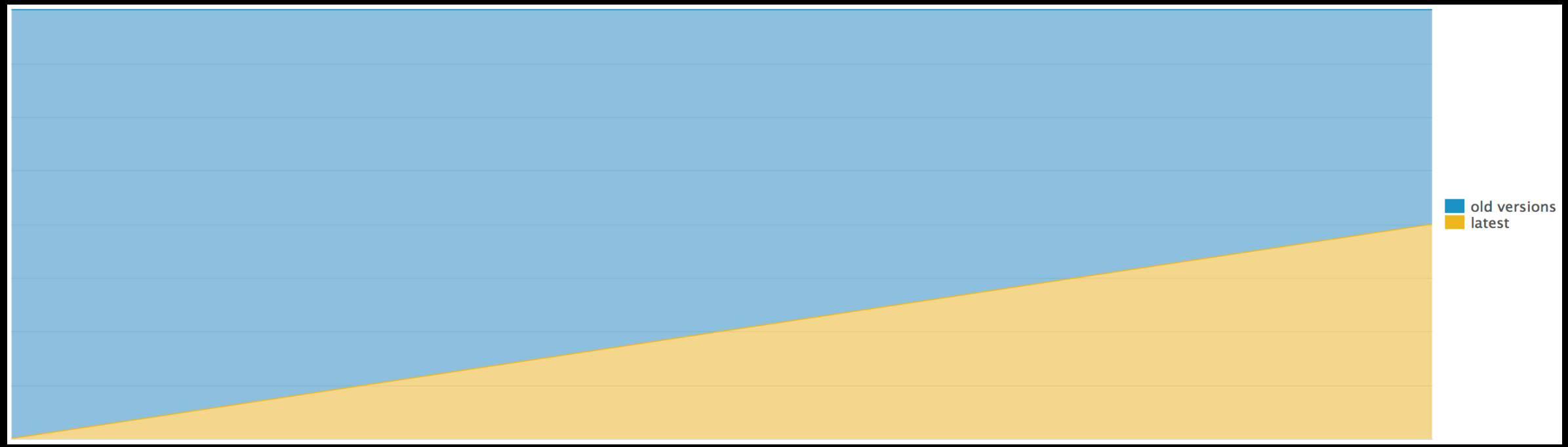
splunk> .conf2017

© 2017 SPLUNK INC.

Renaming groupings in a chart

Summarizing values

- `<search> | eval latest=if(version="1.10","latest","old versions") | timechart count by latest | table _time, "old versions", "latest"`



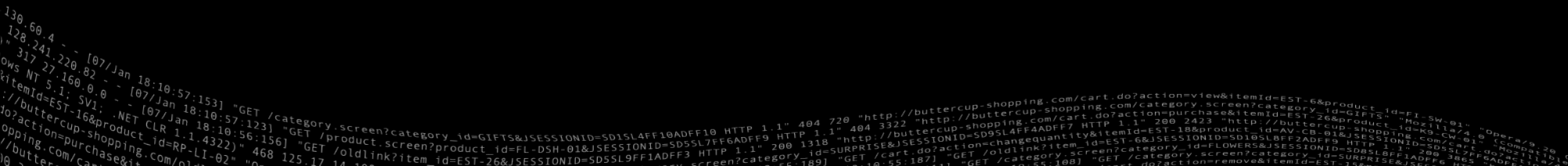
splunk> .conf2017

© 2017 SPLUNK INC.

Renaming groupings in a chart

Adding more detail

- iOS 11 betas report their version as simply “11.0”
- Combine with the networking framework version from user-agent for more granularity
-
```
index=access URL="/v1/logins”
 | rex field=user_agent "
CFNetwork/(?<cfnetwork_version>[.0-9]*) ”
 | eval detailed_ios_version=iosversion."-
".cfnetwork_version
 | top detailed_ios_version
```



splunk> .conf2017

© 2017 SPLUNK INC.

Key Takeaways

1. You can get great data about your client applications from the server logs.
2. Your search query should be as narrow as possible before processing.
3. You should always keep in mind the question you're answering.

© 2017 SPLUNK INC.

Thank You

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