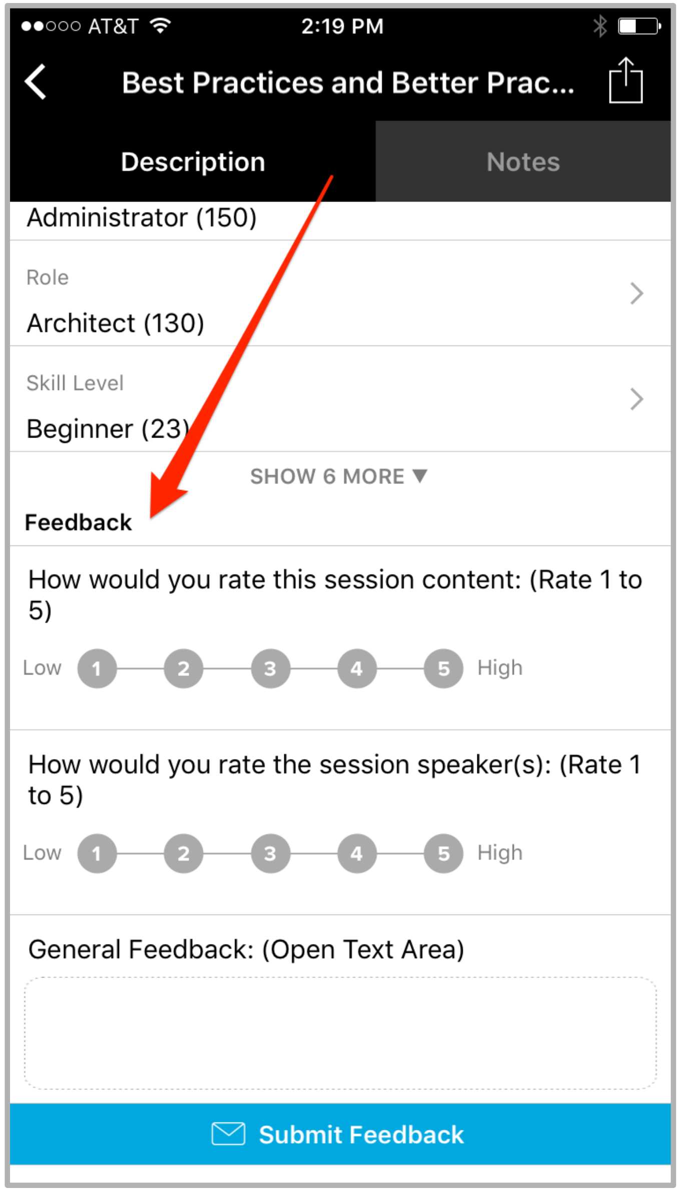
Blueprints for Actionable Alerts

…while you get settled…

- Latest Slides:
  - https://splunk.box.com/v/blueprints-alerts
- Collaborate: #alerting
  - Sign Up @ http://splk.it/slack
- Load Feedback -------------------------------------->



Administrator (150)

Role
Architect (130)

Skill Level
Beginner (23)

SHOW 6 MORE ▼

Feedback

How would you rate this session content: (Rate 1 to 5)

Low ① ② ③ ④ ⑤ High

How would you rate the session speaker(s): (Rate 1 to 5)

Low ① ② ③ ④ ⑤ High

General Feedback: (Open Text Area)

splunk> .conf2017

splunk> .conf2017

Blueprints for Actionable Alerts

Presented by Splunk Blueprints

Burch | Senior Best Practices Engineer

.conf2017 | Version 0.0

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.

“Scale customer success through the automation of adoption services and best practices”

Blueprint’s Mission

What's a "Burch"?

Senior Best Practices Engineer

- Was a Senior Sales Engineer
- Before that, Splunk Customer
- Before that, Middleware Eng
- Before that, Computer Science
- Before that, an idea of my parents

“ From spam to glam with Splunk Alerts”

Should you be here?

splunk> .conf2017

eval Agenda = “Maturity Model”

Very conceptual

1. Stage 1: Message of Concern
2. Stage 2: Thresholds
3. Stage 3: Relative Percentages
4. Stage 4: Average Errors
5. Stage 5: Percentiles
6. Bonus Stage 6: IT Service Intelligence
7. Stage 7: Actionable Alerts

Phase 1: Message of Concern

Attempted Solution

Basic Search => Spammy Alert

```
[Spam]
action.email = true
action.email.to =
welovespam@spam.com
counttype = number of events
cron_schedule = */15 * * * *
dispatch.earliest_time = -15min
dispatch.latest_time = now
enableSched = true
quantity = 0
relation = greater than
search = index=_internal error
```

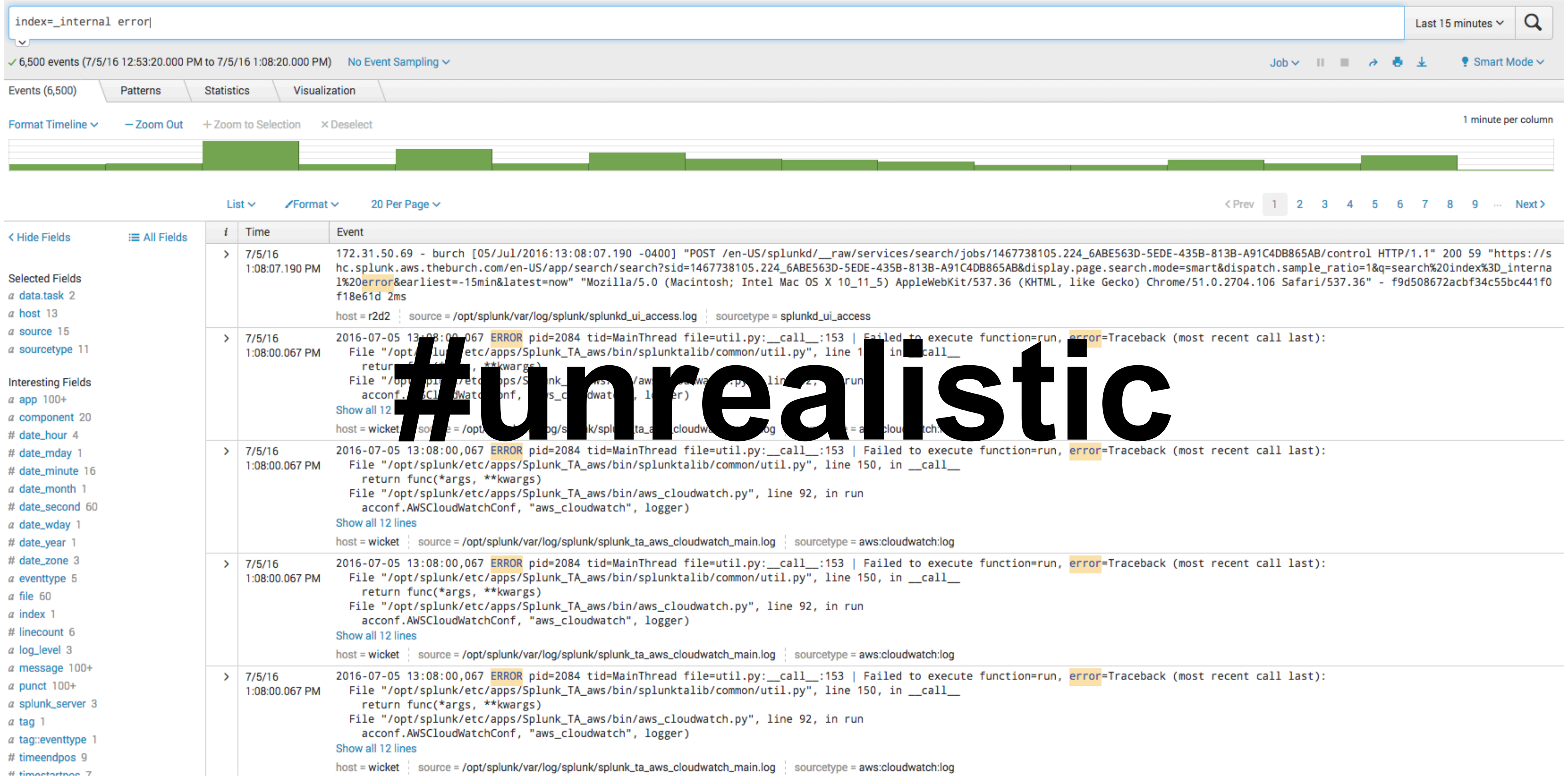
Attempted Solution

Basic Search => Spammy Alert

```
[Spam]
action.email = true
action.email.to =
welovespam@spam.com
counttype = number of events
cron_schedule = */15 * * * *
dispatch.earliest_time = -15min
dispatch.latest_time = now
enableSched = true
quantity = 0
relation = greater than
search = index=_internal error
```

Result

6,500 errors over last 15min



```
index=_internal error
```

Last 15 minutes

✓ 6,500 events (7/5/16 12:53:20.000 PM to 7/5/16 1:08:20.000 PM) No Event Sampling

Job · Smart Mode

Events (6,500) | Patterns | Statistics | Visualization

Format Timeline · — Zoom Out · + Zoom to Selection · × Deselect · 1 minute per column

List · Format · 20 Per Page · ‹ Prev 1 2 3 4 5 6 7 8 9 ... Next ›

‹ Hide Fields · All Fields

Selected Fields
- data.task 2
- host 13
- source 15
- sourcetype 11

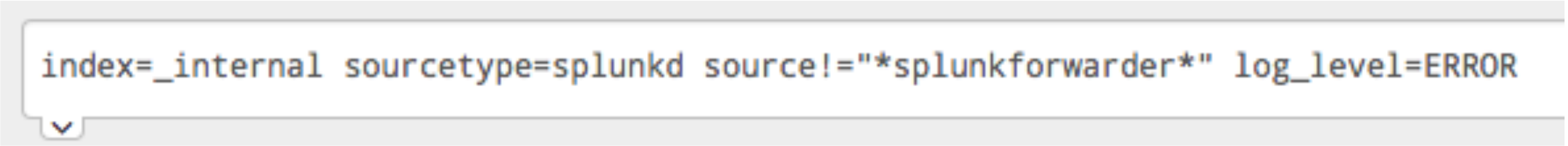
Interesting Fields
- app 100+
- component 20
- date_hour 4
- date_mday 1
- date_minute 16
- date_month 1
- date_second 60
- date_wday 1
- date_year 1
- date_zone 3
- eventtype 5
- file 60
- index 1
- linecount 6
- log_level 3
- message 100+
- punct 100+
- splunk_server 3
- tag 1
- tag::eventtype 1
- timeendpos 9
- timestartpos 7

i	Time	Event
>	7/5/16 1:08:07.190 PM	172.31.50.69 - burch [05/Jul/2016:13:08:07.190 -0400] "POST /en-US/splunkd/__raw/services/search/jobs/1467738105.224_6ABE563D-5EDE-435B-813B-A91C4DB865AB/control HTTP/1.1" 200 59 "https://shc.splunk.aws.theburch.com/en-US/app/search/search?sid=1467738105.224_6ABE563D-5EDE-435B-813B-A91C4DB865AB&display.page.search.mode=smart&dispatch.sample_ratio=1&q=search%20index%3D_internal%20error&earliest=-15min&latest=now" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36" - f9d508672acbf34c55bc441f0f18e61d 2ms host = r2d2 source = /opt/splunk/var/log/splunk/splunkd_ui_access.log sourcetype = splunkd_ui_access
>	7/5/16 1:08:00.067 PM	2016-07-05 13:[illegible]067 ERROR pid=2084 tid=MainThread file=util.py:__call__:153 | [illegible] execute function=run, error=Traceback (most recent call last): File "/opt[illegible]etc/apps/Splunk_TA_aws/bin/splunktalib/common/util.py", line 1[illegible] in[illegible]call__ retur[illegible], **kwargs) File "/[illegible] acconf.[illegible] Show all 12 [illegible] host = wicket [illegible]
>	7/5/16 1:08:00.067 PM	2016-07-05 13:08:00,067 ERROR pid=2084 tid=MainThread file=util.py:__call__:153 | Failed to execute function=run, error=Traceback (most recent call last): File "/opt/splunk/etc/apps/Splunk_TA_aws/bin/splunktalib/common/util.py", line 150, in __call__ return func(*args, **kwargs) File "/opt/splunk/etc/apps/Splunk_TA_aws/bin/aws_cloudwatch.py", line 92, in run acconf.AWSCloudWatchConf, "aws_cloudwatch", logger) Show all 12 lines host = wicket source = /opt/splunk/var/log/splunk/splunk_ta_aws_cloudwatch_main.log sourcetype = aws:cloudwatch:log
>	7/5/16 1:08:00.067 PM	2016-07-05 13:08:00,067 ERROR pid=2084 tid=MainThread file=util.py:__call__:153 | Failed to execute function=run, error=Traceback (most recent call last): File "/opt/splunk/etc/apps/Splunk_TA_aws/bin/splunktalib/common/util.py", line 150, in __call__ return func(*args, **kwargs) File "/opt/splunk/etc/apps/Splunk_TA_aws/bin/aws_cloudwatch.py", line 92, in run acconf.AWSCloudWatchConf, "aws_cloudwatch", logger) Show all 12 lines host = wicket source = /opt/splunk/var/log/splunk/splunk_ta_aws_cloudwatch_main.log sourcetype = aws:cloudwatch:log
>	7/5/16 1:08:00.067 PM	2016-07-05 13:08:00,067 ERROR pid=2084 tid=MainThread file=util.py:__call__:153 | Failed to execute function=run, error=Traceback (most recent call last): File "/opt/splunk/etc/apps/Splunk_TA_aws/bin/splunktalib/common/util.py", line 150, in __call__ return func(*args, **kwargs) File "/opt/splunk/etc/apps/Splunk_TA_aws/bin/aws_cloudwatch.py", line 92, in run acconf.AWSCloudWatchConf, "aws_cloudwatch", logger) Show all 12 lines host = wicket source = /opt/splunk/var/log/splunk/splunk_ta_aws_cloudwatch_main.log sourcetype = aws:cloudwatch:log

#unrealistic

Obvious Improvements

- Scope of problem is large
  - Solution: indexed fields (index, source, sourcetype, and/or pattern)
- Problem: “error” matches more than desired
  - Solution: bind with fields like log_level="error”
- Result: Stronger search ignores benign results

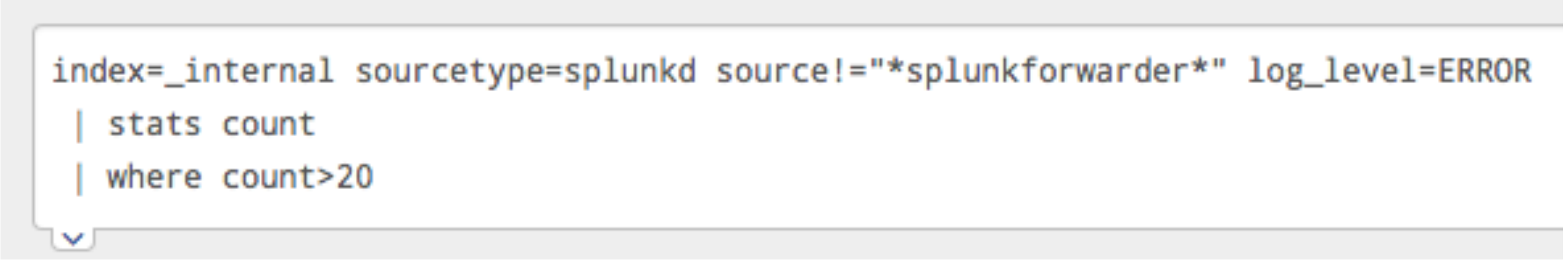


```
index=_internal sourcetype=splunkd source!="*splunkforwarder*" log_level=ERROR
```

Phase 2: Thresholds

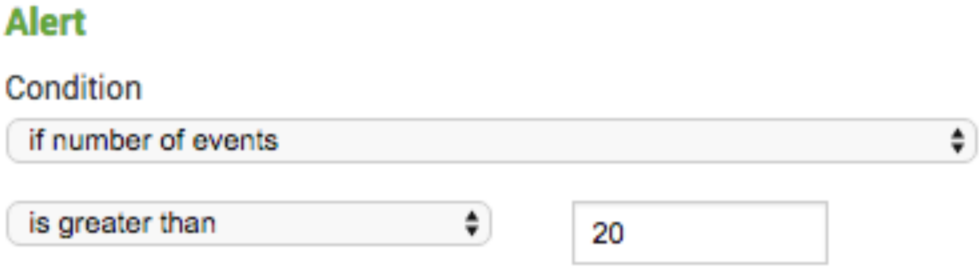
Attempted Solution

- Only alert if more than “arbitrary” # occurrences / time
  - Arbitrary = perception of healthy



```
index=_internal sourcetype=splunkd source!="*splunkforwarder*" log_level=ERROR
 | stats count
 | where count>20
```

  - or…



Alert

Condition

if number of events

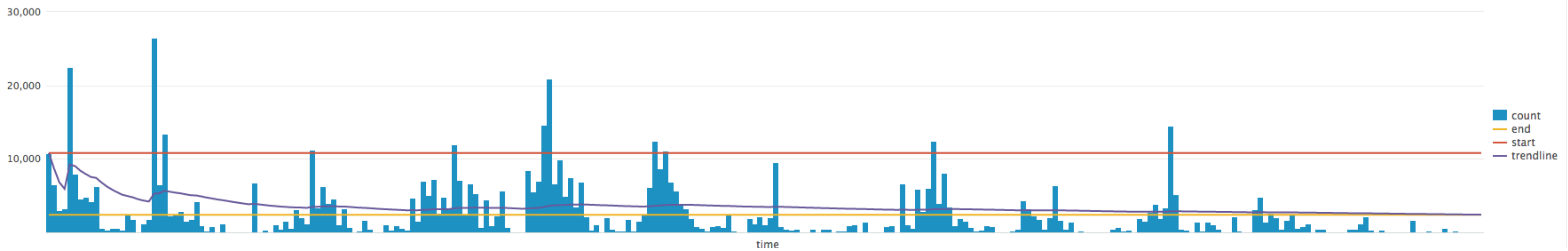
is greater than

20

Result & Obvious Improvements

- Ignores variances of different types of errors
  - Web errors rarely happen but server errors happen often

- Fluctuations relative to usage
  - Threshold too small or large during peak or minimal usage, respectively
  - Static thresholds not adjusting with business growth or decline



Phase 3:
Relative Percentages

What 2 Clean?

Ingredients: Pork with Ham, Salt, Water, Modified Potato Starch, Sugar, Sodium Nitrite
SPAM®
Classic
U.S. INSPECTED AND PASSED BY DEPARTMENT OF AGRICULTURE
Serving Suggestion
NET WT 12 OZ (340g)

© London Media

New Concept

eval goal_attacking = coalesce(spam, system)

Spam

- Normalize against # of errors
- Ignore non error events
- log_level=ERROR

- Good for clean up
- Bad for permanent

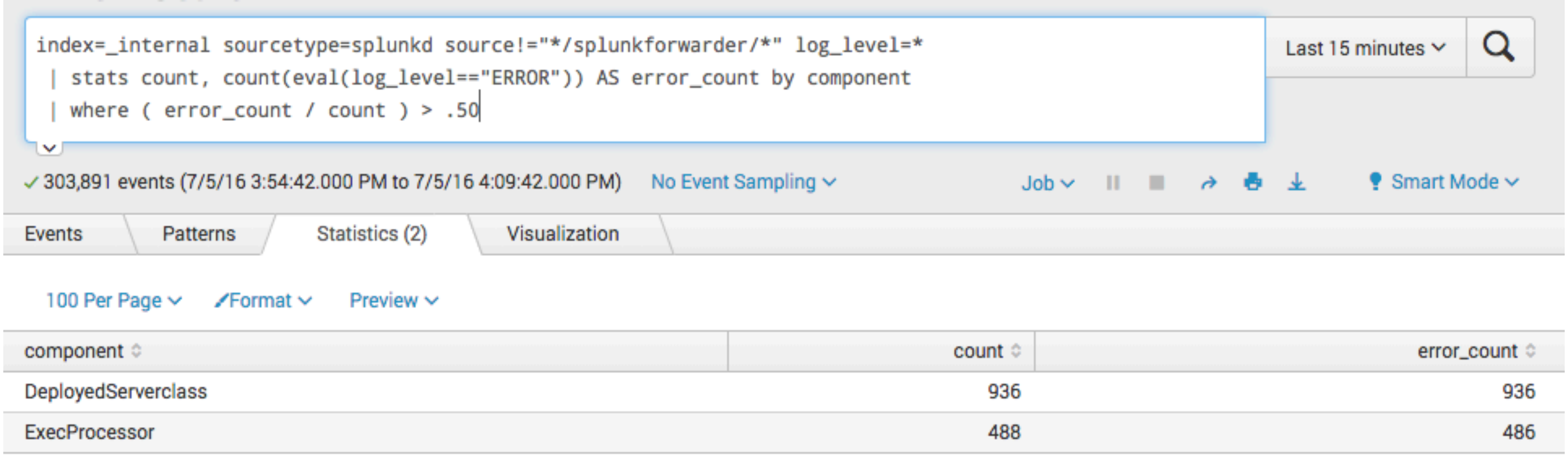
System

- Normalize to all events
- Include all error + non error events
- log_level=*

- Good for permanent
- Bad for clean up

Attempted Solution

Large % Items



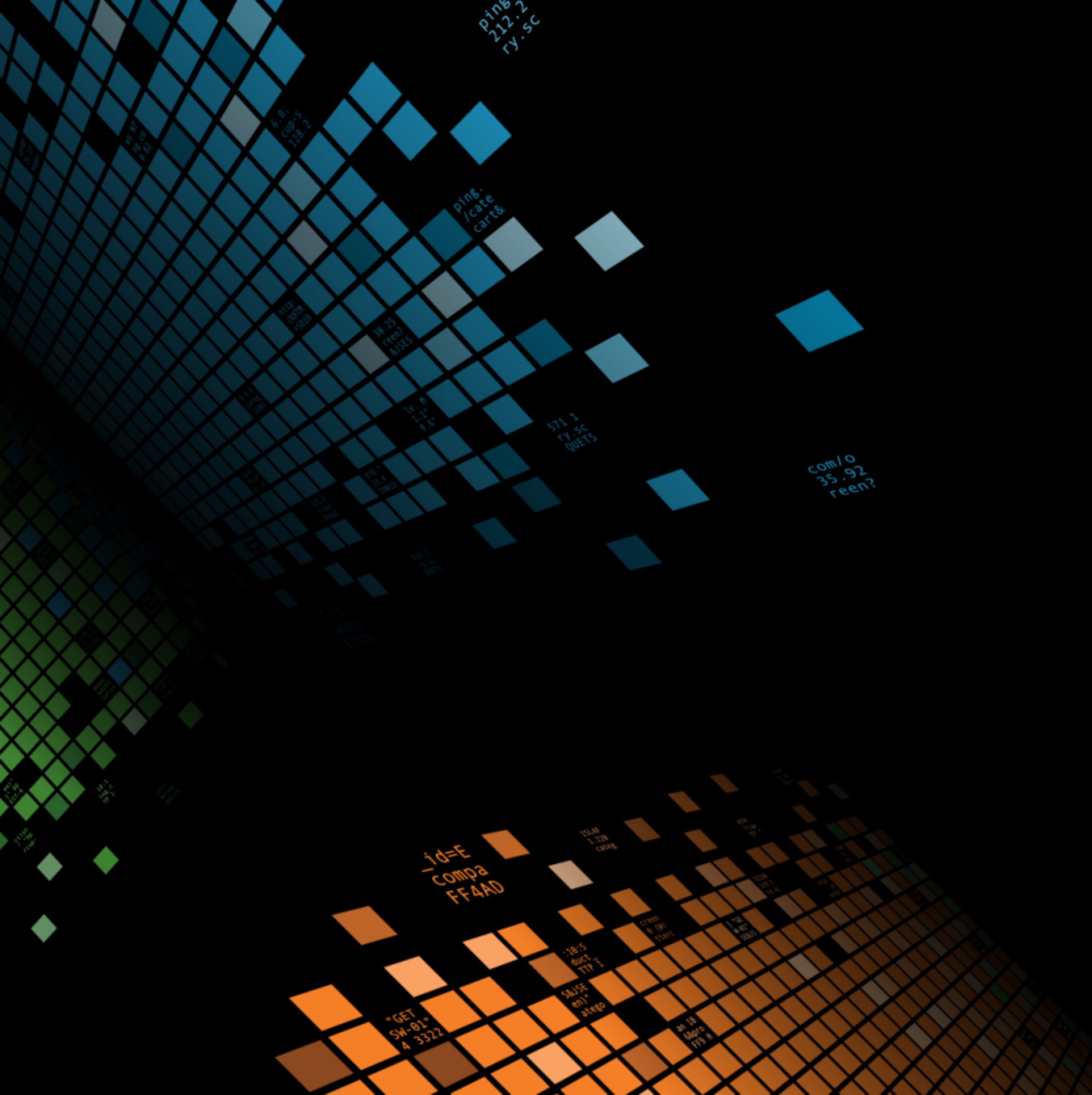
```
index=_internal sourcetype=splunkd source!="*/splunkforwarder/*" log_level=*
 | stats count, count(eval(log_level=="ERROR")) AS error_count by component
 | where ( error_count / count ) > .50
```

✓ 303,891 events (7/5/16 3:54:42.000 PM to 7/5/16 4:09:42.000 PM)

component	count	error_count
DeployedServerclass	936	936
ExecProcessor	488	486

Result & Obvious Improvements

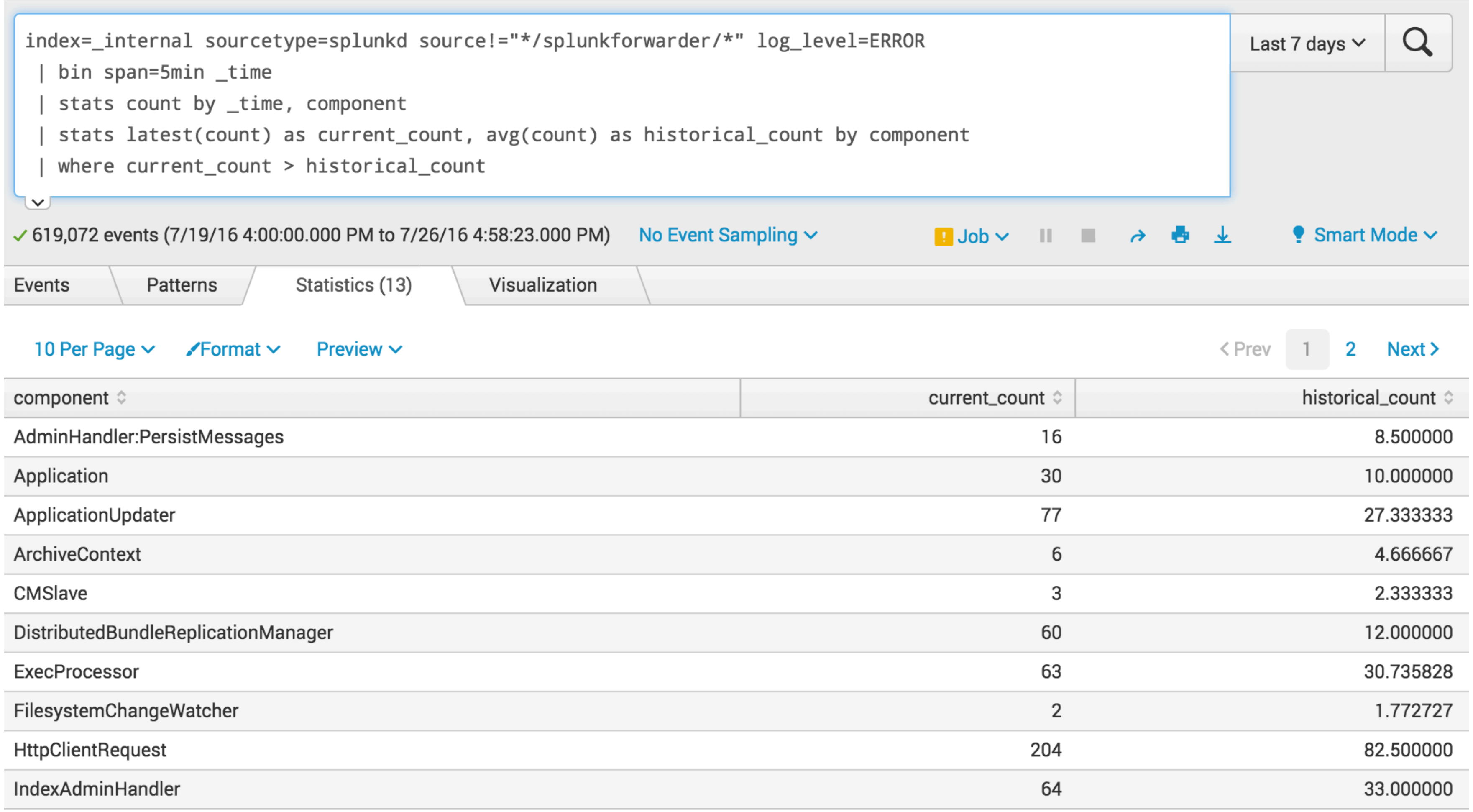
- Huge improvement
  - Less spam
  - Adjusts because normalized to volume
- What if that’s normal?
  - Then persistent alerts that should be ignored = spam + noise!
- Percentage => Static => Arbitrary?!



Phase 4:
Average Errors

Attempted Solution

Current period vs historical average



```
index=_internal sourcetype=splunkd source!="*/splunkforwarder/*" log_level=ERROR
 | bin span=5min _time
 | stats count by _time, component
 | stats latest(count) as current_count, avg(count) as historical_count by component
 | where current_count > historical_count
```

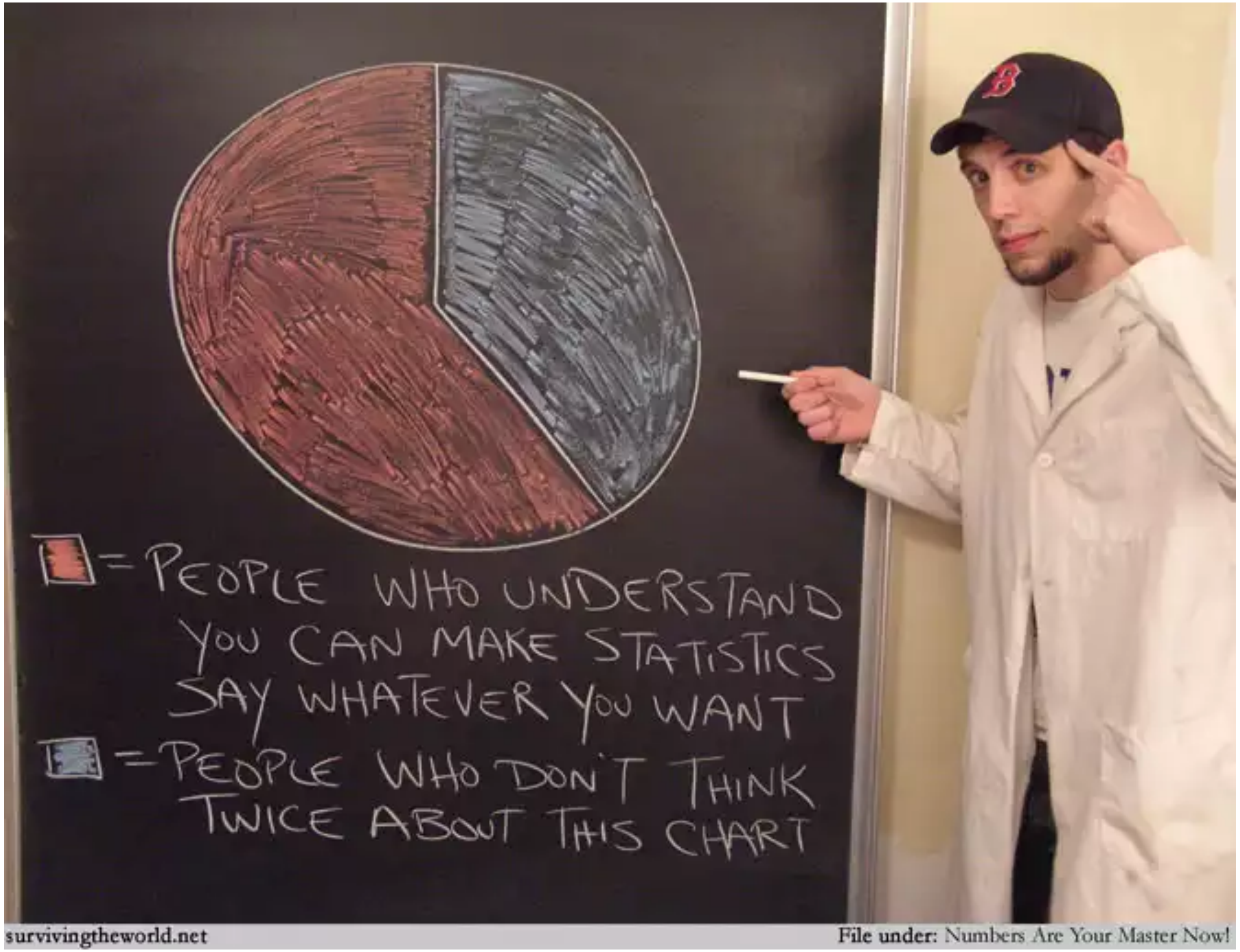
✓ 619,072 events (7/19/16 4:00:00.000 PM to 7/26/16 4:58:23.000 PM)

component	current_count	historical_count
AdminHandler:PersistMessages	16	8.500000
Application	30	10.000000
ApplicationUpdater	77	27.333333
ArchiveContext	6	4.666667
CMSlave	3	2.333333
DistributedBundleReplicationManager	60	12.000000
ExecProcessor	63	30.735828
FilesystemChangeWatcher	2	1.772727
HttpClientRequest	204	82.500000
IndexAdminHandler	64	33.000000

Result

- Adjusts with changes in environment!
- Slow
  - Summary Indexing?
  - Acceleration?
- How often alert?
  - Definition of average!

Statistics Detour


🟥 = PEOPLE WHO UNDERSTAND YOU CAN MAKE STATISTICS SAY WHATEVER YOU WANT
🟦 = PEOPLE WHO DON'T THINK TWICE ABOUT THIS CHART

survivingtheworld.net

File under: Numbers Are Your Master Now!

Statistics Detour

Historical # of errors / 5 min period

11

31

56

87

5

67

19

54000

21

18

77

Statistics Detour

11

31

56

87

5

67

19

54000

21

18

77

0 to 10 | 11 to 20 | 21 to 29 | 30 to 39 | 40 to 49 | 50 to 59 | 60 to 69 | 70 to 79 | 80 to 89 | 90 to 99

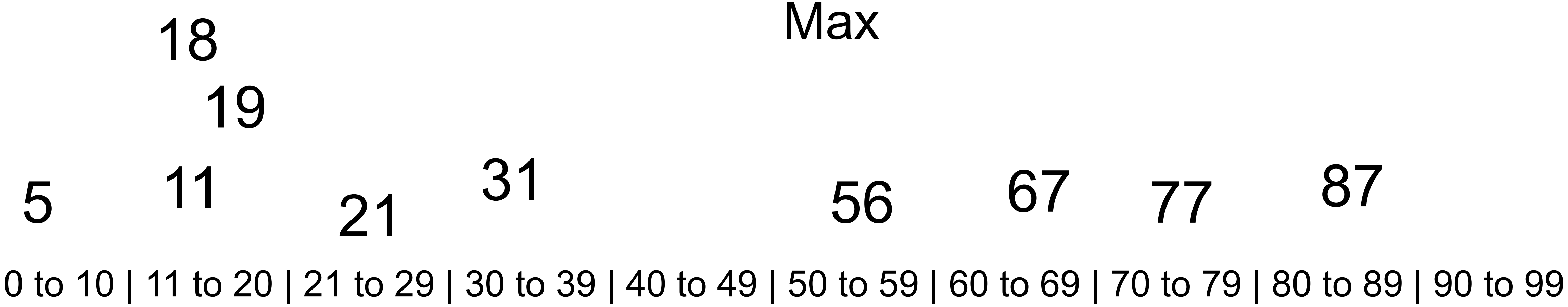
Statistics Detour

At what value does this become actionable?

Min

Average

Max



18

19

5

11

21

31

56

67

77

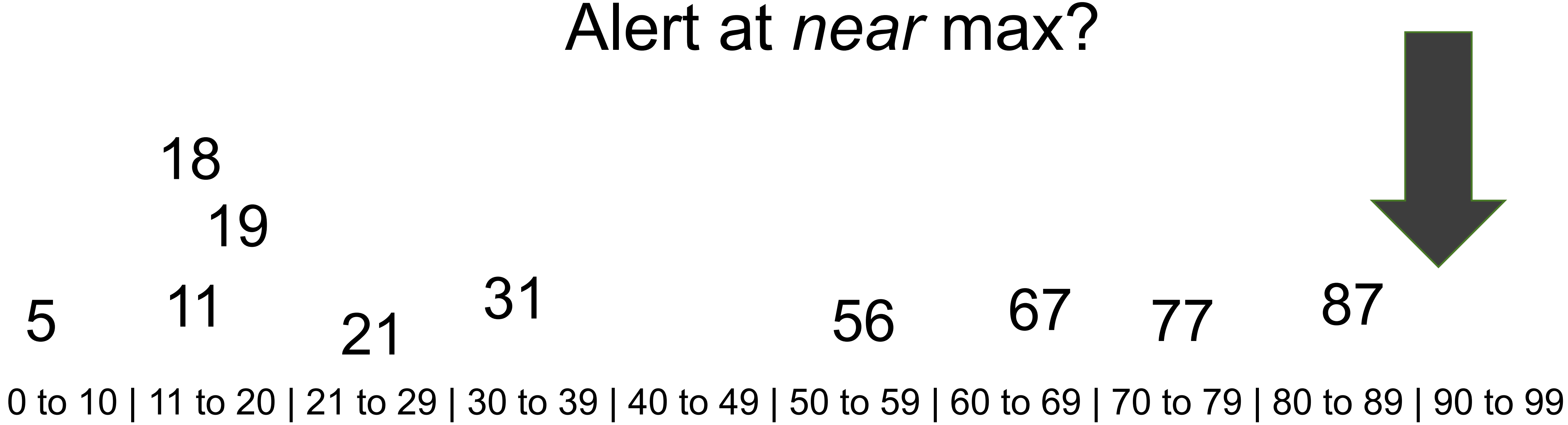
87

0 to 10 | 11 to 20 | 21 to 29 | 30 to 39 | 40 to 49 | 50 to 59 | 60 to 69 | 70 to 79 | 80 to 89 | 90 to 99

Statistics Detour

What if we could skim off outliers?

Alert at *near* max?



18

19

5 11 21 31 56 67 77 87

0 to 10 | 11 to 20 | 21 to 29 | 30 to 39 | 40 to 49 | 50 to 59 | 60 to 69 | 70 to 79 | 80 to 89 | 90 to 99

Statistics Detour

perc<X>(Y) = Returns the X-th percentile value of the numeric field Y, where X is an integer between 1 and 99. The percentile X-th function **sorts the values** of Y in an increasing order. Then, if you consider that 0% is the **lowest** and 100% the **highest**, the functions picks the **value that corresponds to the position** of the X% value.

18

19

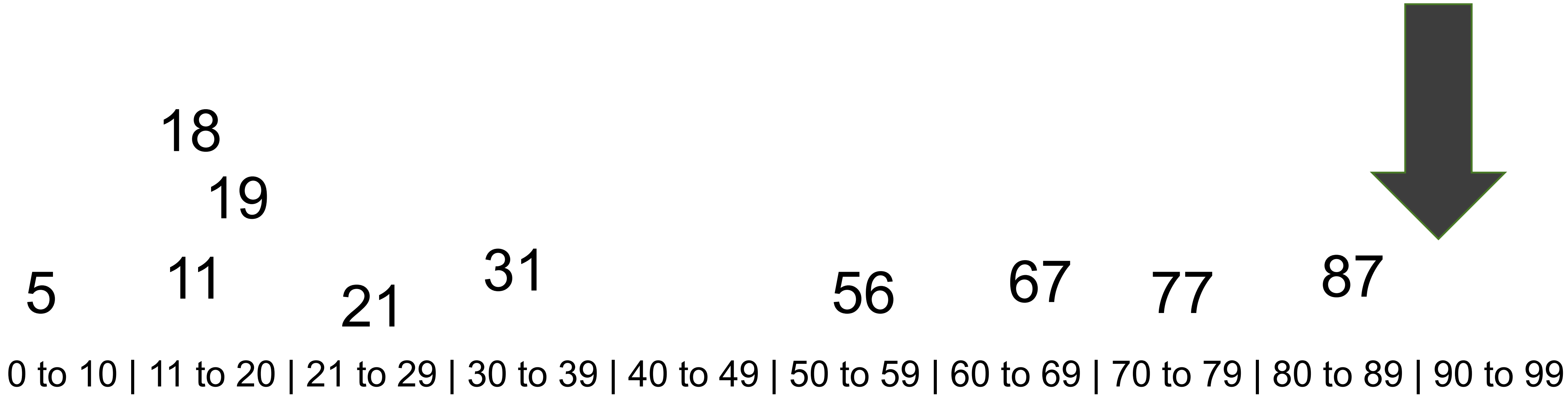
5 11 21 31 56 67 77 87

0 to 10 | 11 to 20 | 21 to 29 | 30 to 39 | 40 to 49 | 50 to 59 | 60 to 69 | 70 to 79 | 80 to 89 | 90 to 99

splunk> .conf2017

Statistics Detour

perc90(this_result_set) = ?



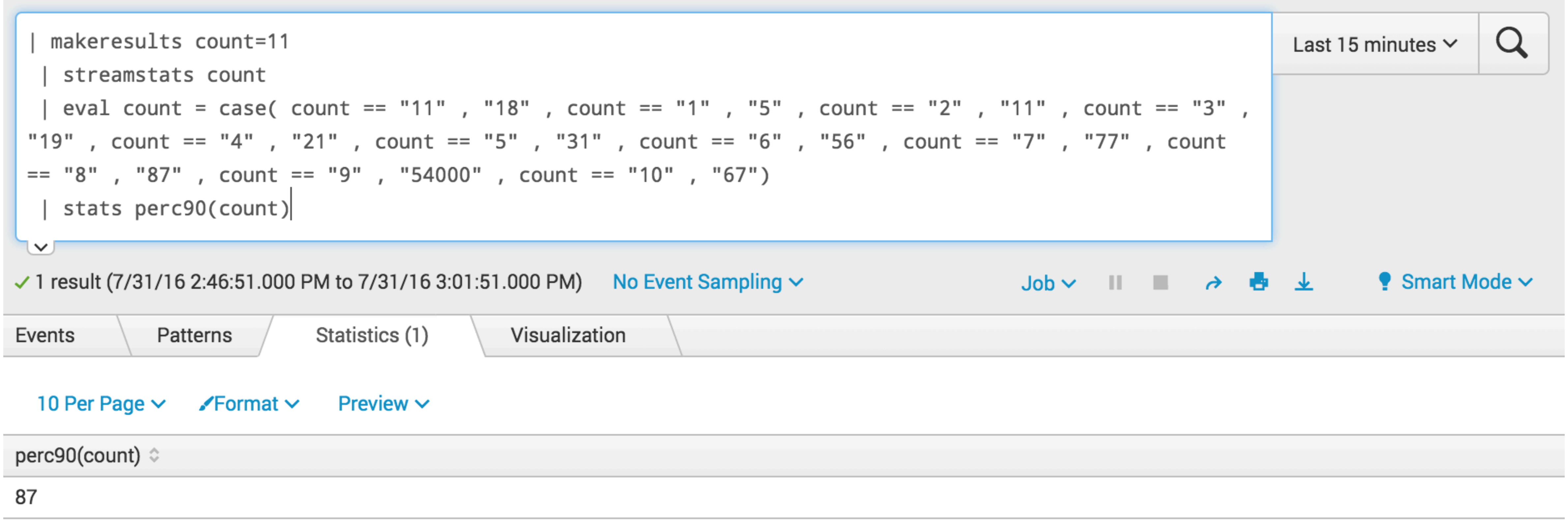
18

19

5 11 21 31 56 67 77 87

0 to 10 | 11 to 20 | 21 to 29 | 30 to 39 | 40 to 49 | 50 to 59 | 60 to 69 | 70 to 79 | 80 to 89 | 90 to 99

Statistics Detour

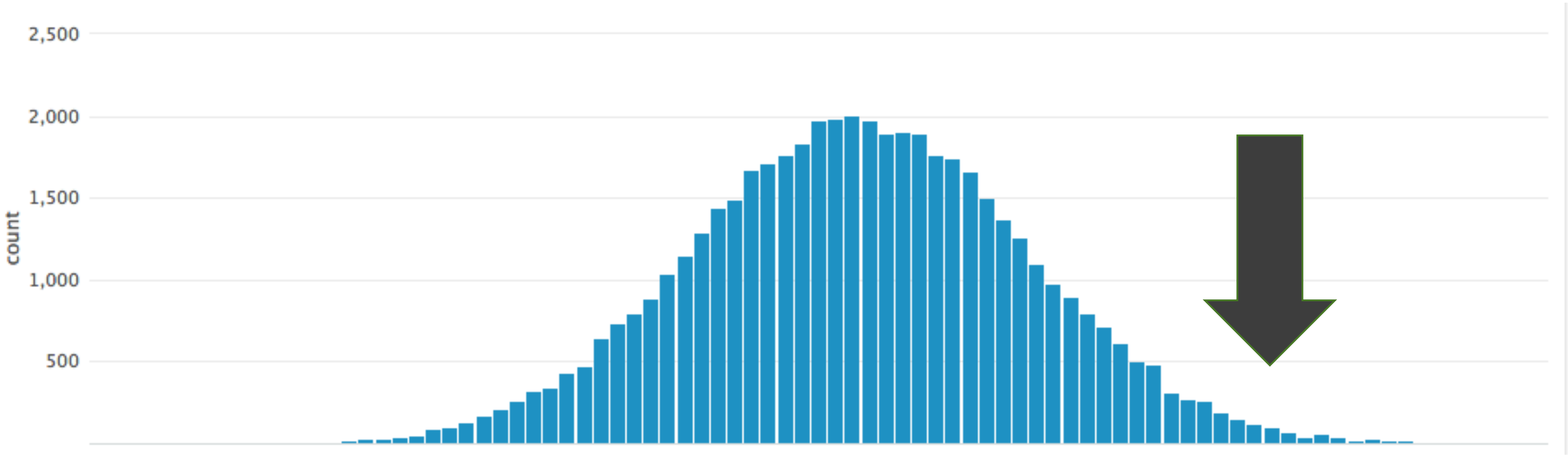


```
| makeresults count=11
 | streamstats count
 | eval count = case( count == "11" , "18" , count == "1" , "5" , count == "2" , "11" , count == "3" ,
"19" , count == "4" , "21" , count == "5" , "31" , count == "6" , "56" , count == "7" , "77" , count
== "8" , "87" , count == "9" , "54000" , count == "10" , "67")
 | stats perc90(count)
```

✓ 1 result (7/31/16 2:46:51.000 PM to 7/31/16 3:01:51.000 PM)

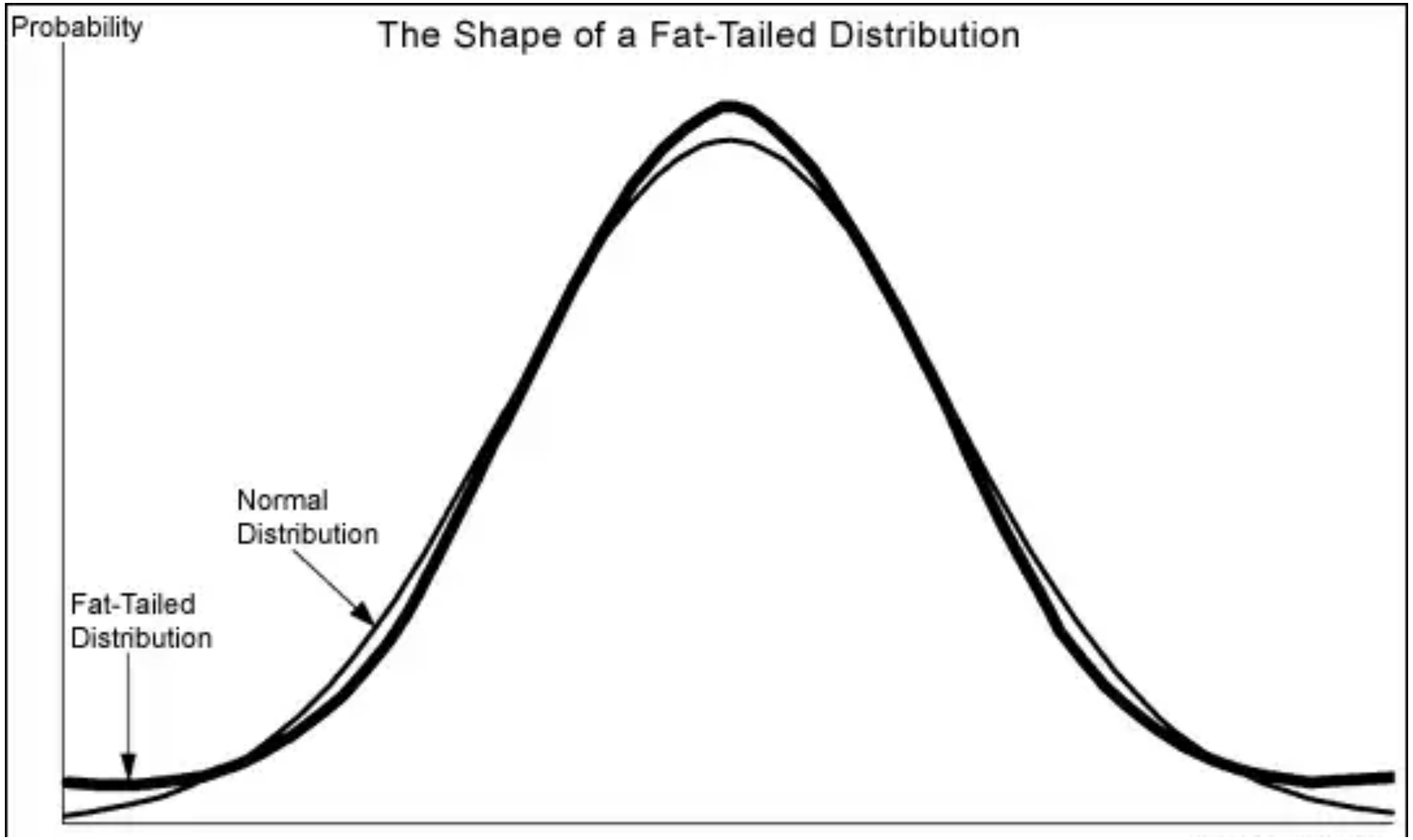
perc90(count)
87

Warning: Assumption

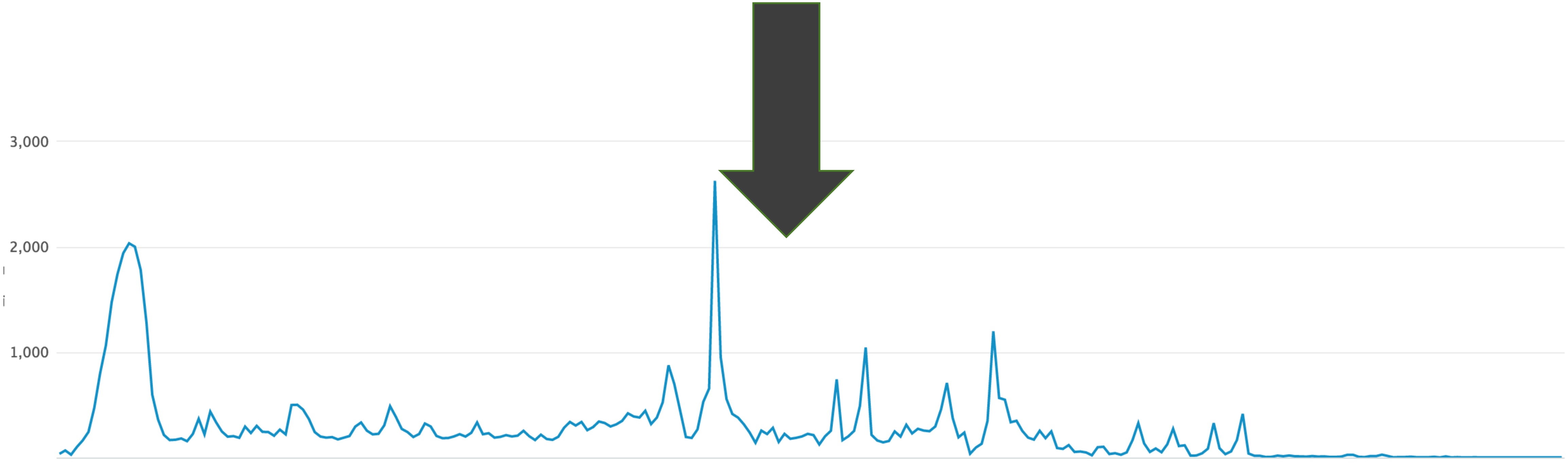


Shout out to Xander!

Warning: Heavy Tails



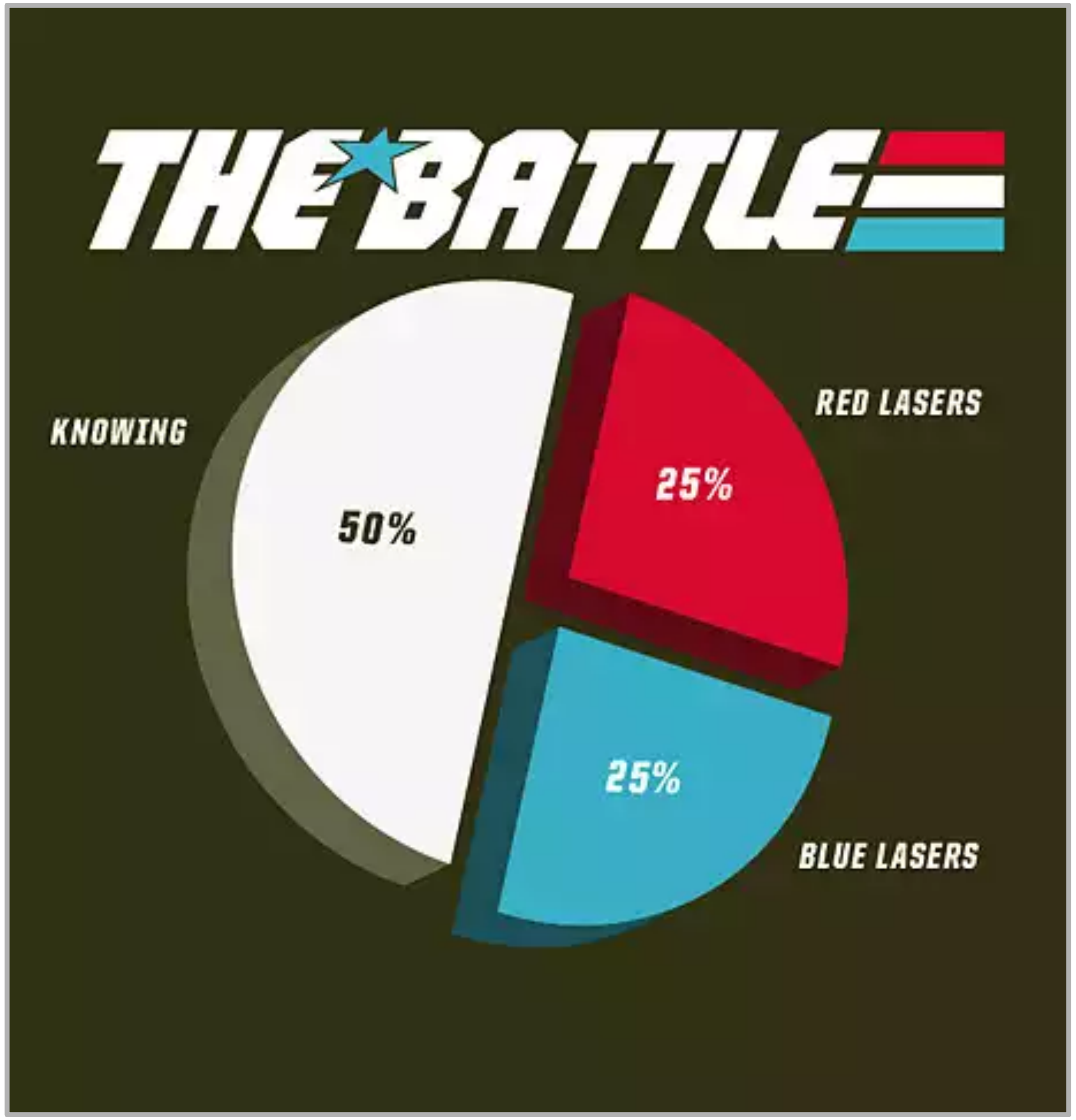
Warning: Reality

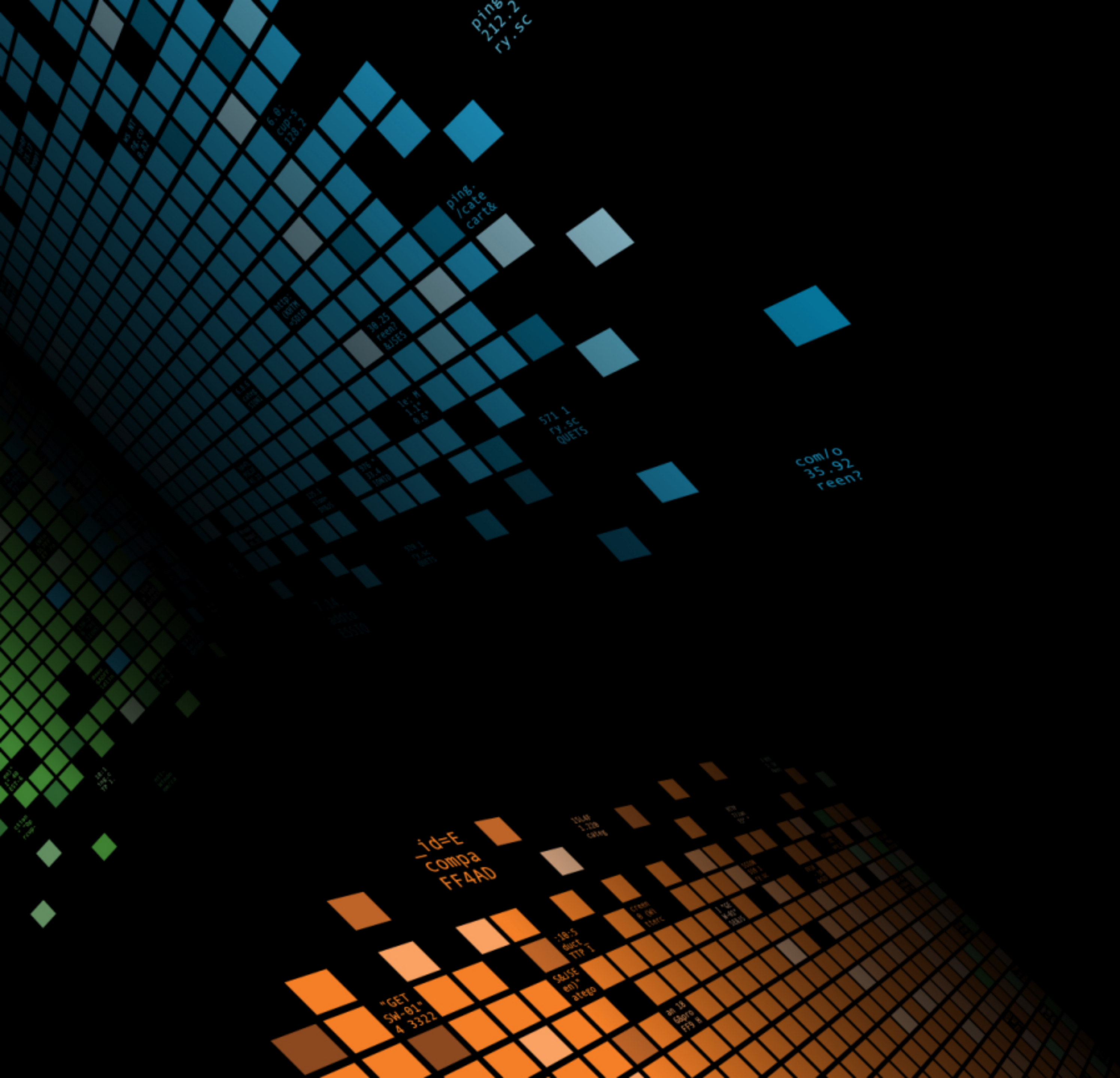


What percentile is appropriate given this distribution?

Know Thy Data

```
index=_internal sourcetype=splunkd
source!="*/splunkforwarder/*”
  | bin span=5min _time
  | stats count AS group by _time
  | bin span=1000 group
  | stats count by group
  | sort group
```





Phase 5: Percentiles

Attempted Solution

- Current period’s error rate vs. historical error rate
  - by error category (component)

```
index=_internal sourcetype=splunkd source!="*/splunkforwarder/*"
log_level=ERROR
  | bin span=5min _time
  | stats count by _time, component
  | stats perc95(count) AS perc95_count, latest(count) AS current_count
by component
  | where current_count > perc95_count
```

- Performance?

Summary Indexing Solution

- Generate malleable historical data

```
index=_internal sourcetype=splunkd source!="*/splunkforwarder/*"
log_level=ERROR
 | bin span=5min _time
 | sistats count by _time, component
```

- Alert upon historical data

```
index=summary_internal sourcetype=stash source="my search name”
 | stats count by _time, component
 | stats perc95(count) AS perc95_count, latest(count) AS current_count
by component
```

The Lasso Approach

- Triage Strategy
- Perimeter around errors
- Tighten lasso by reducing percentile
- Rinse & repeat

Alternatives

- Address most common errors first
  - Start at 5th percentile and work up

- Normalization Frames:
  - Same errors
  - All errors
  - All events
  - Time windows (e.g. work hours)

Result

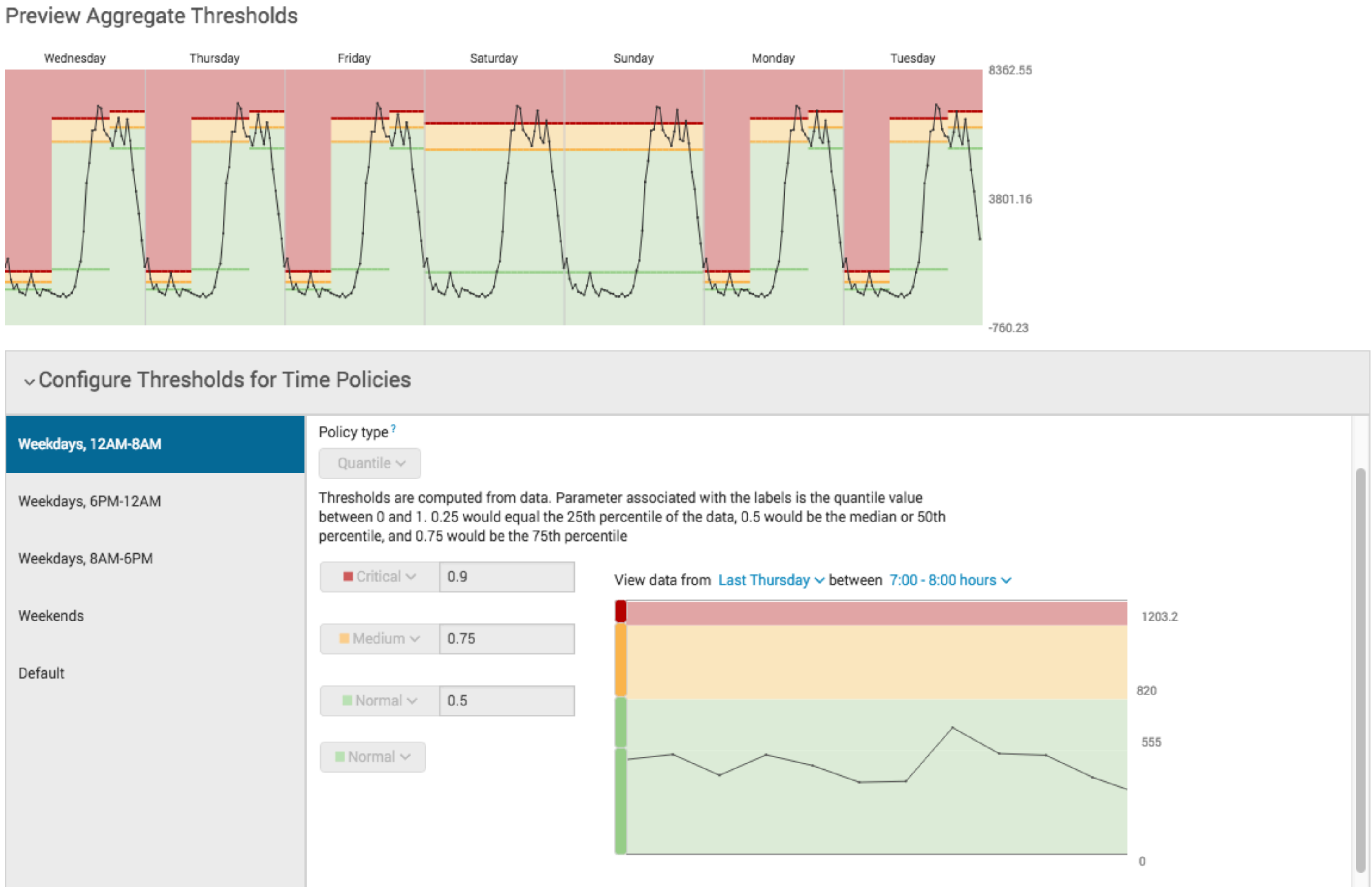
- Adjusts with changes in environment!
- Requires Maintenance
  - Power User skillz
  - Summary Indexing
- Not period time adjusted
  - Fluctuations in business day or period

Bonus Phase 6: IT Service Intelligence

“Make alerting accessible, usable and valuable to everyone!”

Why ITSI?

Quantile, Range, and STDDEV. Oh my!



Preview Aggregate Thresholds

Configure Thresholds for Time Policies

- Weekdays, 12AM-8AM
- Weekdays, 6PM-12AM
- Weekdays, 8AM-6PM
- Weekends
- Default

Policy type ?

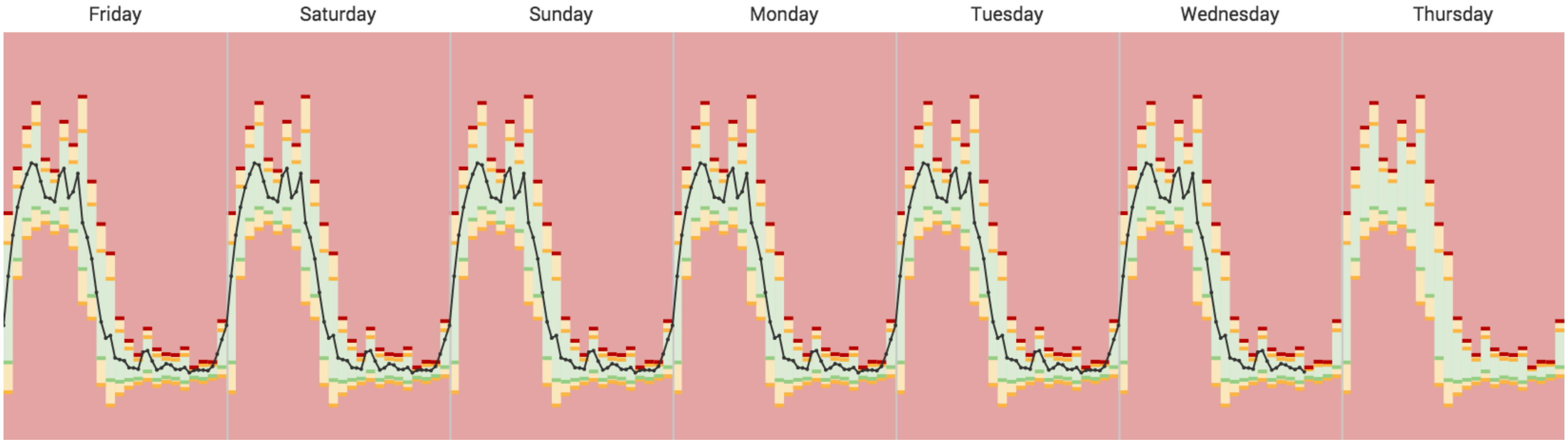
Quantile

Thresholds are computed from data. Parameter associated with the labels is the quantile value between 0 and 1. 0.25 would equal the 25th percentile of the data, 0.5 would be the median or 50th percentile, and 0.75 would be the 75th percentile

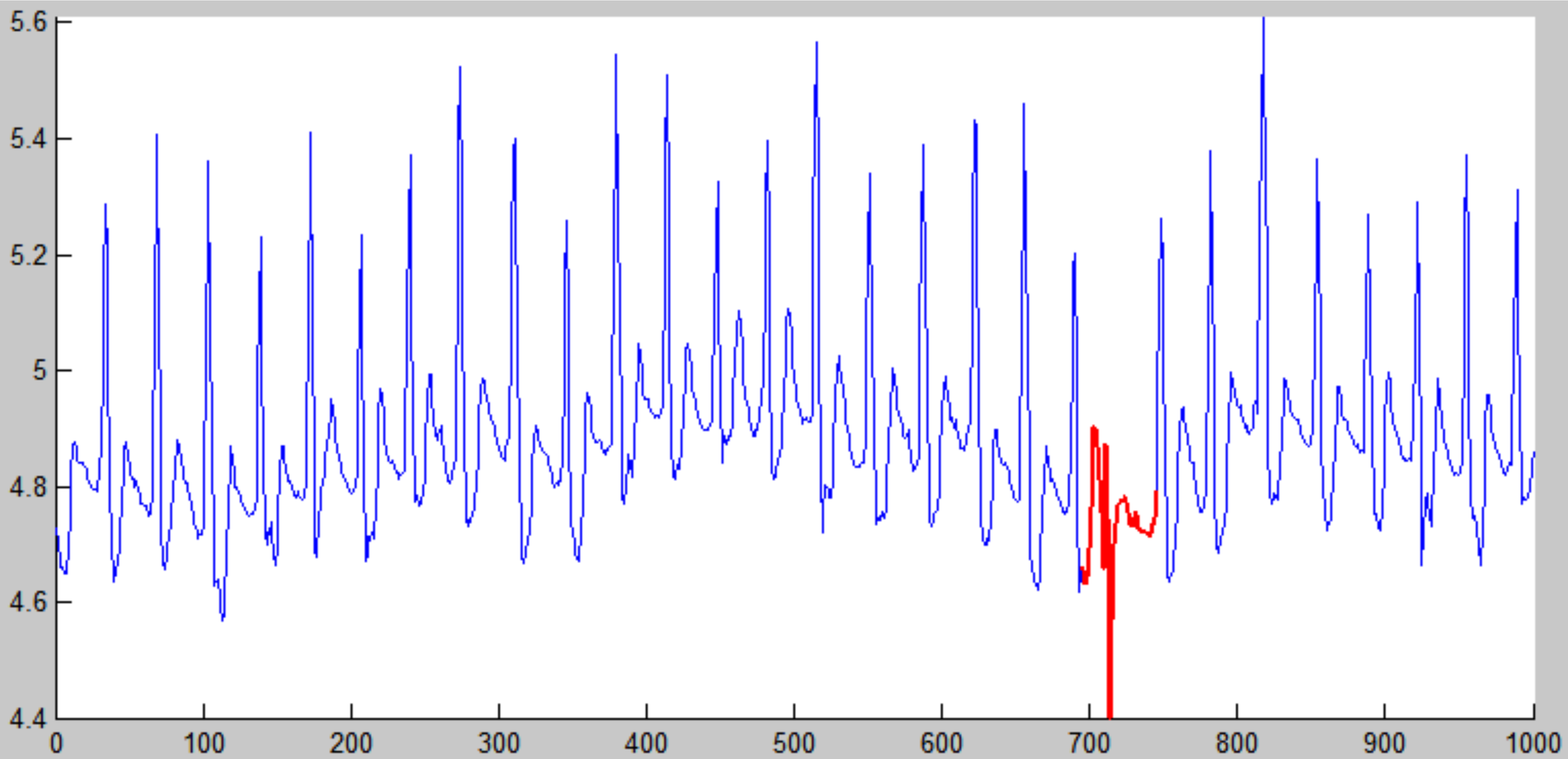
🟥 Critical	0.9
🟧 Medium	0.75
🟩 Normal	0.5
🟩 Normal	

View data from Last Thursday between 7:00 - 8:00 hours

Adaptive Thresholds

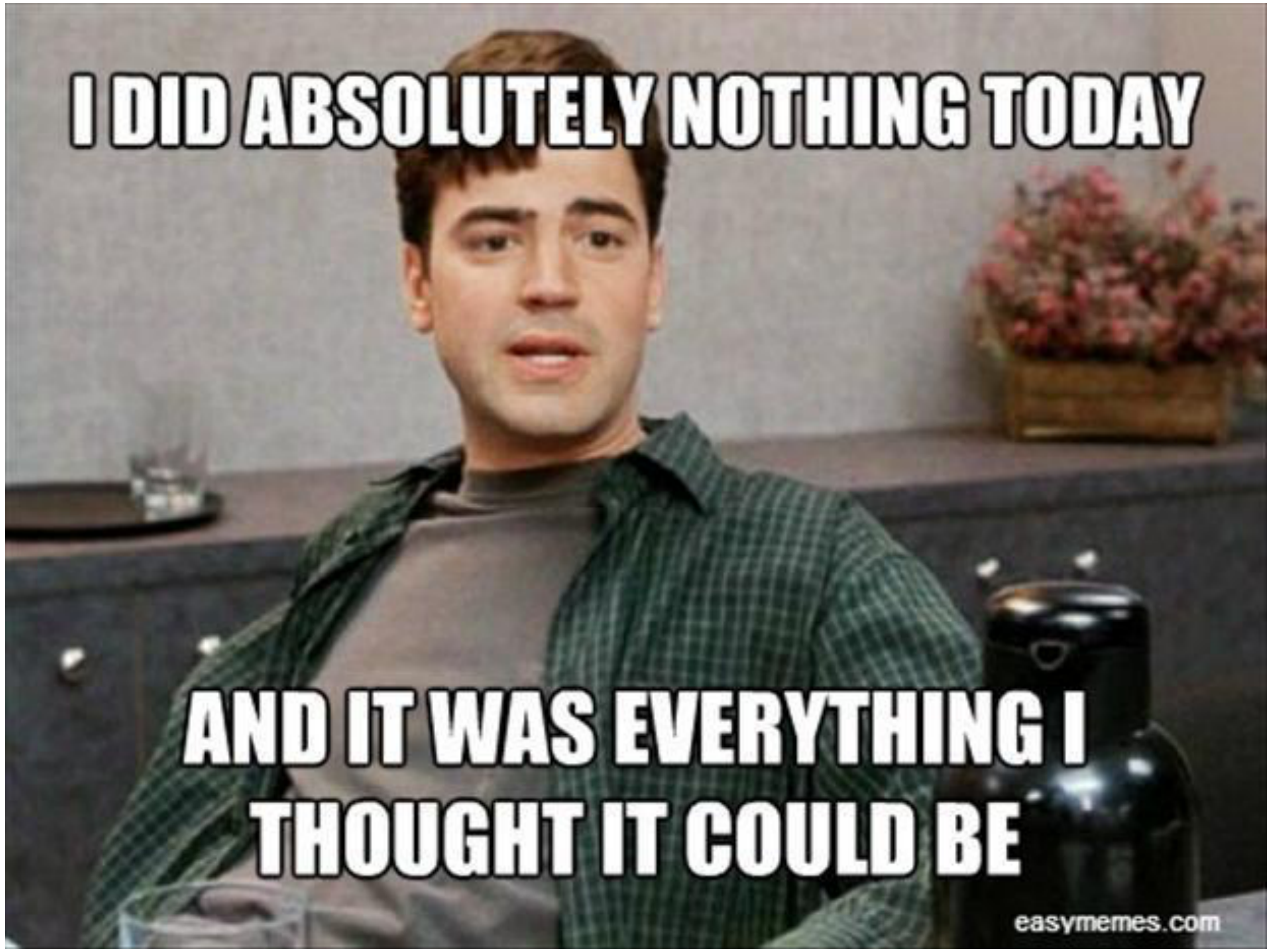


Anomaly Detection



Phase 7: Actionable Alerts

Actionable Alerts Made Easy


I DID ABSOLUTELY NOTHING TODAY
AND IT WAS EVERYTHING I THOUGHT IT COULD BE
easymemes.com

Wrap Up

1. Stage 1: Message of Concern
2. Stage 2: Thresholds
3. Stage 3: Relative Percentages
4. Stage 4: Average Errors
5. Stage 5: Percentiles
6. Bonus Stage 6: IT Service Intelligence
7. Stage 7: Actionable Alerts

What Now?

Related breakout sessions and activities…

8DEC0D

1. Rate this! (be honest)
2. Collaborate: #alerting
   - Sign Up @ http://splk.it/slack
3. Customer Success Studio
4. More talks, search for
   - Blueprints
   - Burch
   - Champagne
   - Delaney
   - Optimization
   - Best Practices
   - Veuve

splunk> .conf2017

Questions & Discussion?

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

splunk> .conf2017