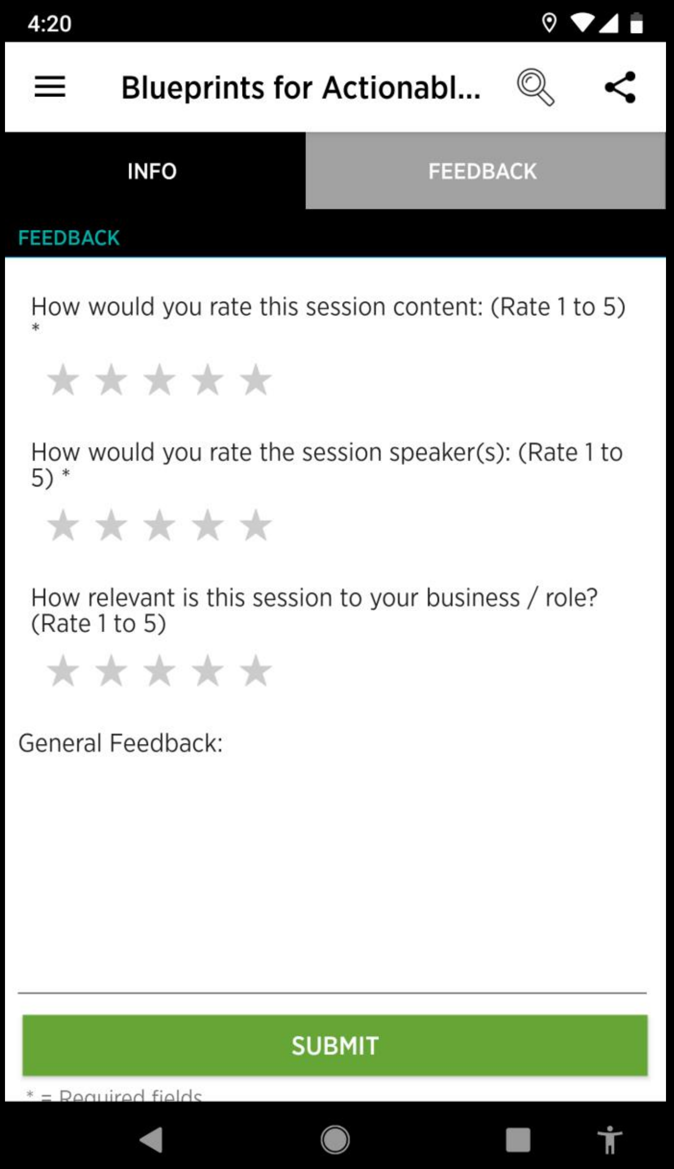
Blueprints for Actionable Alerts

…while you get settled…

- Latest Slides:
  - https://splunk.box.com/v/conf18-alerts
- Collaborate: #alerting
  - Sign Up @ http://splk.it/slack
- Load Feedback ------------------------>



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

★ ★ ★ ★ ★

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

★ ★ ★ ★ ★

How relevant is this session to your business / role? (Rate 1 to 5)

★ ★ ★ ★ ★

General Feedback:

* = Required fields

Blueprints for Actionable Alerts

“From spam to glam with Splunk Alerts”

Burch | Manager, Product Best Practices

.conf18 > Presented by Splunk’s Digital Customer Success

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's a "Burch"?

Manager, Product Best Practices

- Education: Comp Sci + MBA
- Werk: Middleware Eng

- Splunk Customer since 2012
  - Admin for four environments
  - This is based on a true story…

- Splunk Employee since 2014
  - Sales Engineer
  - Best Practices Engineer
  - "Best Practiced Deployment" (CoE)

eval Agenda = "Maturity Model"

weak --> strong

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
```

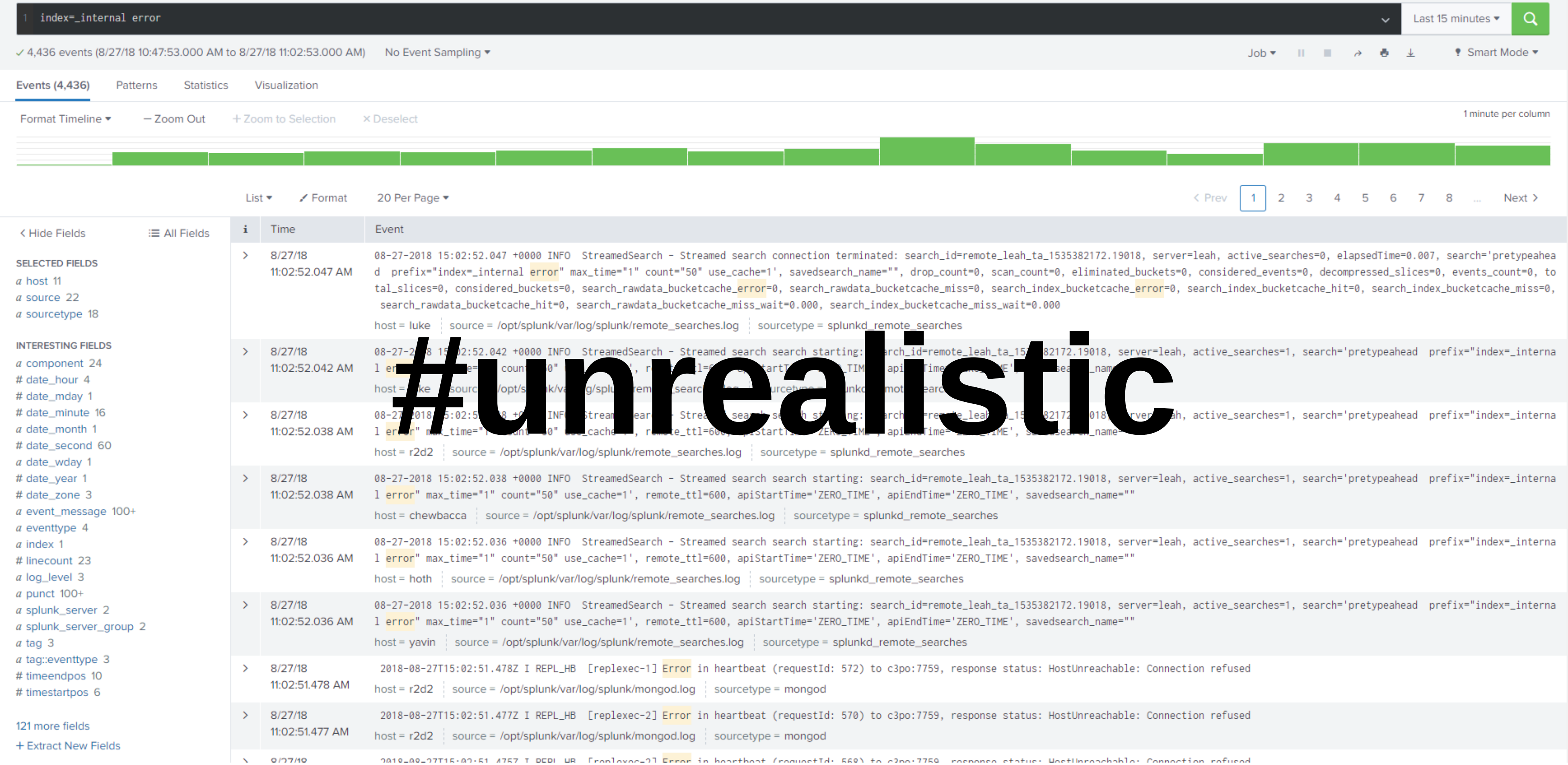
Attempted Solution

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

4,436 errors over last 15min



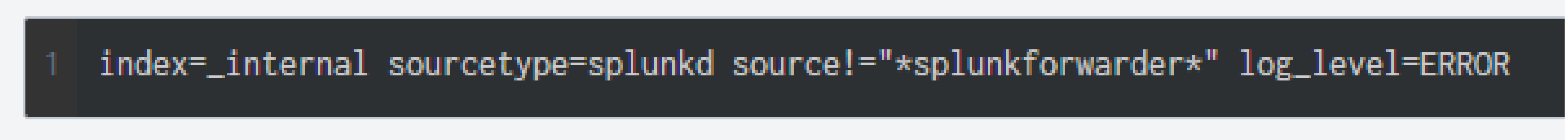
i	Time	Event
›	8/27/18 11:02:52.047 AM	08-27-2018 15:02:52.047 +0000 INFO StreamedSearch - Streamed search connection terminated: search_id=remote_leah_ta_1535382172.19018, server=leah, active_searches=0, elapsedTime=0.007, search='pretypeahead prefix="index=_internal error" max_time="1" count="50" use_cache=1', savedsearch_name="", drop_count=0, scan_count=0, eliminated_buckets=0, considered_events=0, decompressed_slices=0, events_count=0, total_slices=0, considered_buckets=0, search_rawdata_bucketcache_error=0, search_rawdata_bucketcache_miss=0, search_index_bucketcache_error=0, search_index_bucketcache_hit=0, search_index_bucketcache_miss=0, search_rawdata_bucketcache_hit=0, search_rawdata_bucketcache_miss_wait=0.000, search_index_bucketcache_miss_wait=0.000 host = luke ┆ source = /opt/splunk/var/log/splunk/remote_searches.log ┆ sourcetype = splunkd_remote_searches
›	8/27/18 11:02:52.042 AM	08-27-2 8 15 2:52.042 +0000 INFO StreamedSearch - Streamed search starting: arch_id=remote_leah_ta_15 82172.19018, server=leah, active_searches=1, search='pretypeahead prefix="index=_internal er e= count 0" ', r tl=6 startT TIM api Time ME', sea nam host = ke sourc /opt/s nk/va g/splu rem searc urcetype nkd mot earc
›	8/27/18 11:02:52.038 AM	08-27 2018 5:02:5 8 +0 INF Stream ear Stre sea se h st ng: arch =remote_leah 15 82172 018 rver ah, active_searches=1, search='pretypeahead prefix="index=_internal error" max_time="1 ount 0" use_cache 1', remote_ttl=600, apiStartTi ZERO_TIME', apiEndTime= ZERO_TIME', savedsearch_name= host = r2d2 ┆ source = /opt/splunk/var/log/splunk/remote_searches.log ┆ sourcetype = splunkd_remote_searches
›	8/27/18 11:02:52.038 AM	08-27-2018 15:02:52.038 +0000 INFO StreamedSearch - Streamed search search starting: search_id=remote_leah_ta_1535382172.19018, server=leah, active_searches=1, search='pretypeahead prefix="index=_internal error" max_time="1" count="50" use_cache=1', remote_ttl=600, apiStartTime='ZERO_TIME', apiEndTime='ZERO_TIME', savedsearch_name="" host = chewbacca ┆ source = /opt/splunk/var/log/splunk/remote_searches.log ┆ sourcetype = splunkd_remote_searches
›	8/27/18 11:02:52.036 AM	08-27-2018 15:02:52.036 +0000 INFO StreamedSearch - Streamed search search starting: search_id=remote_leah_ta_1535382172.19018, server=leah, active_searches=1, search='pretypeahead prefix="index=_internal error" max_time="1" count="50" use_cache=1', remote_ttl=600, apiStartTime='ZERO_TIME', apiEndTime='ZERO_TIME', savedsearch_name="" host = hoth ┆ source = /opt/splunk/var/log/splunk/remote_searches.log ┆ sourcetype = splunkd_remote_searches
›	8/27/18 11:02:52.036 AM	08-27-2018 15:02:52.036 +0000 INFO StreamedSearch - Streamed search search starting: search_id=remote_leah_ta_1535382172.19018, server=leah, active_searches=1, search='pretypeahead prefix="index=_internal error" max_time="1" count="50" use_cache=1', remote_ttl=600, apiStartTime='ZERO_TIME', apiEndTime='ZERO_TIME', savedsearch_name="" host = yavin ┆ source = /opt/splunk/var/log/splunk/remote_searches.log ┆ sourcetype = splunkd_remote_searches
›	8/27/18 11:02:51.478 AM	2018-08-27T15:02:51.478Z I REPL_HB [replexec-1] Error in heartbeat (requestId: 572) to c3po:7759, response status: HostUnreachable: Connection refused host = r2d2 ┆ source = /opt/splunk/var/log/splunk/mongod.log ┆ sourcetype = mongod
›	8/27/18 11:02:51.477 AM	2018-08-27T15:02:51.477Z I REPL_HB [replexec-2] Error in heartbeat (requestId: 570) to c3po:7759, response status: HostUnreachable: Connection refused host = r2d2 ┆ source = /opt/splunk/var/log/splunk/mongod.log ┆ sourcetype = mongod

#unrealistic

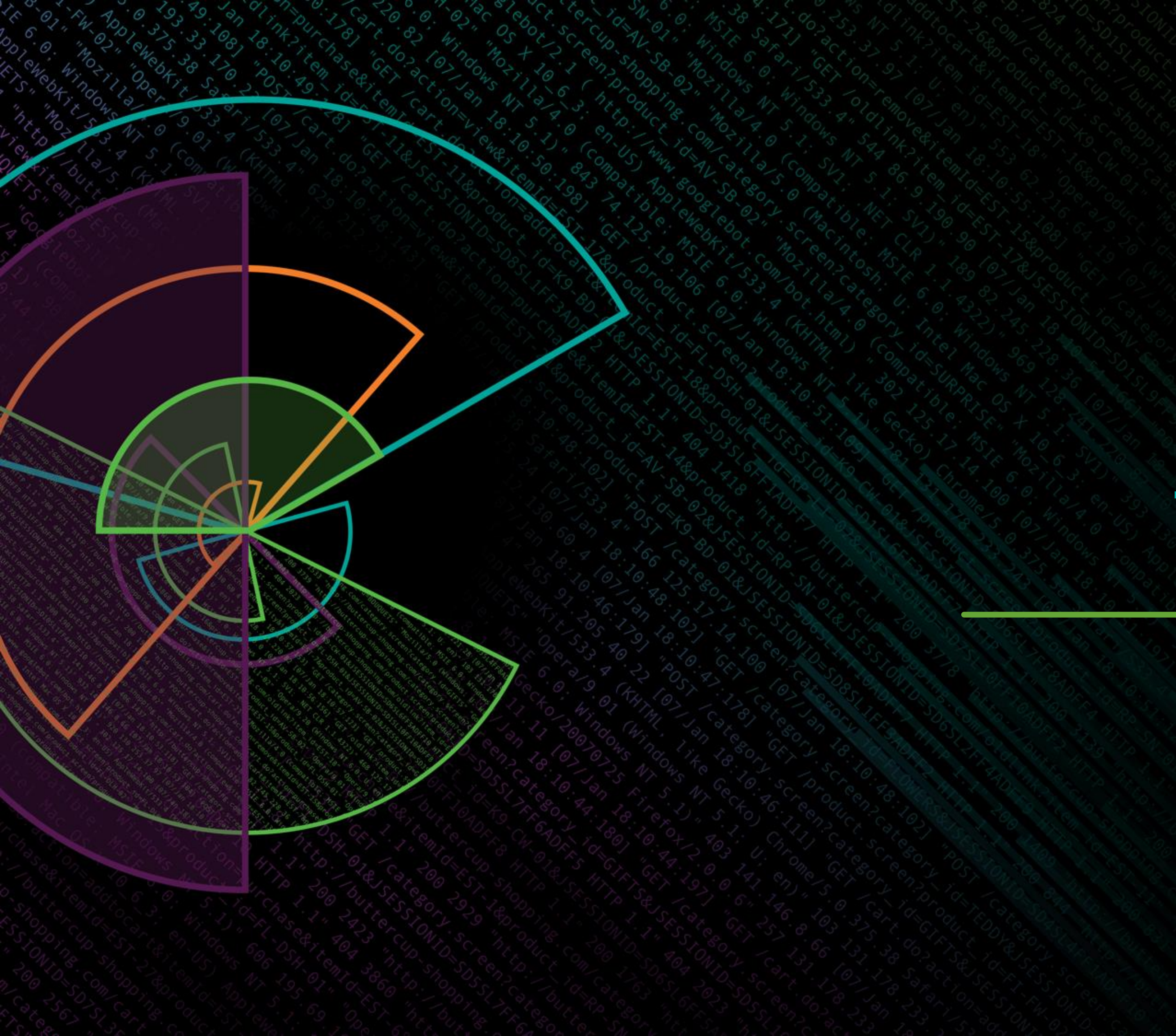
Message > Thresholds > Relative % > Averages > Percentiles > ITSI > Actionable Alerts

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



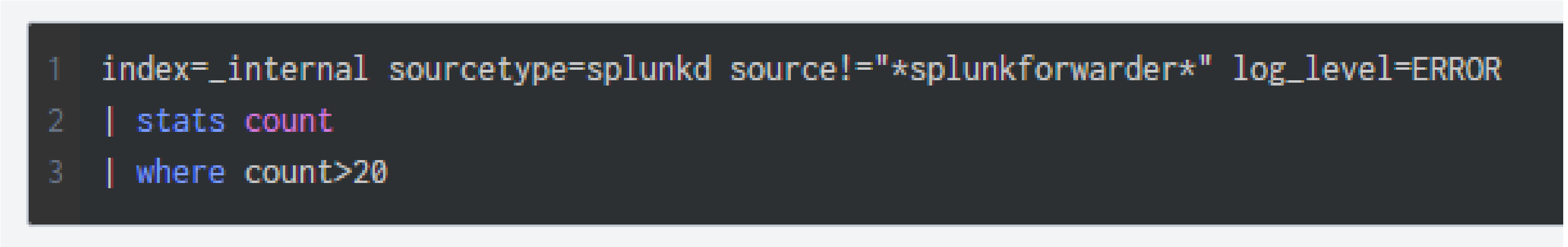
```
index=_internal sourcetype=splunkd source!="*splunkforwarder*" log_level=ERROR
```



Phase 2: Thresholds

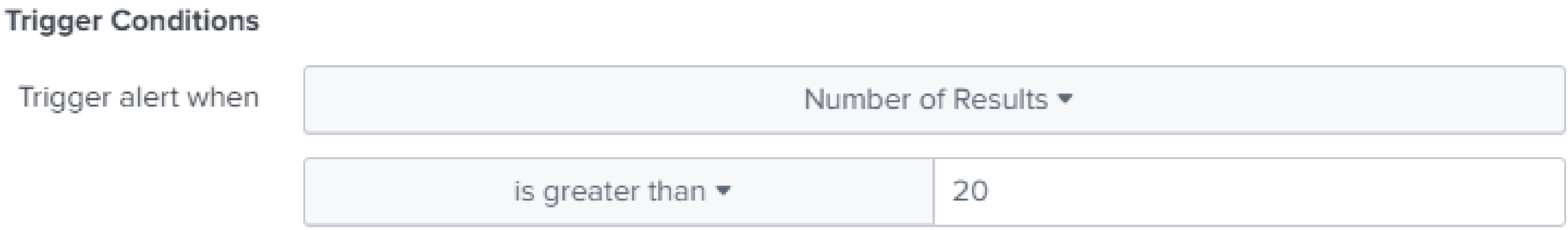
Attempted Solution

- 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…



Trigger Conditions

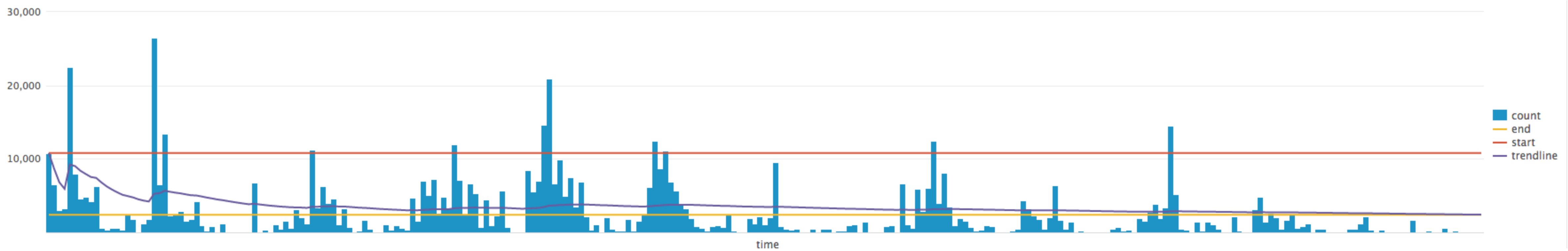
Trigger alert when: Number of Results ▾

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

Message > Thresholds > **Relative %** > Averages > Percentiles > ITSI > Actionable Alerts

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

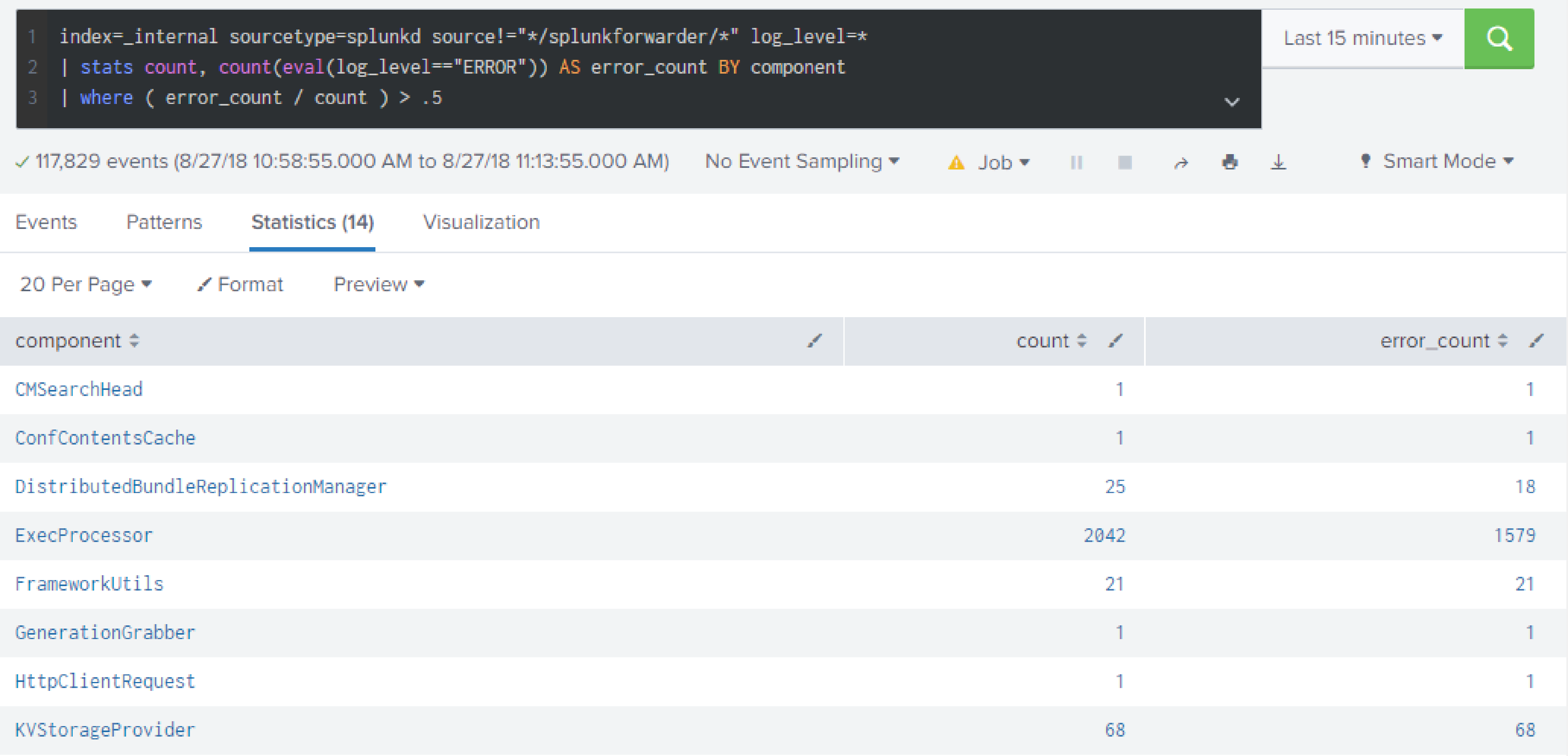
System

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

- Good for permanent
- Bad for clean up

Attempted Solution

Large % Items



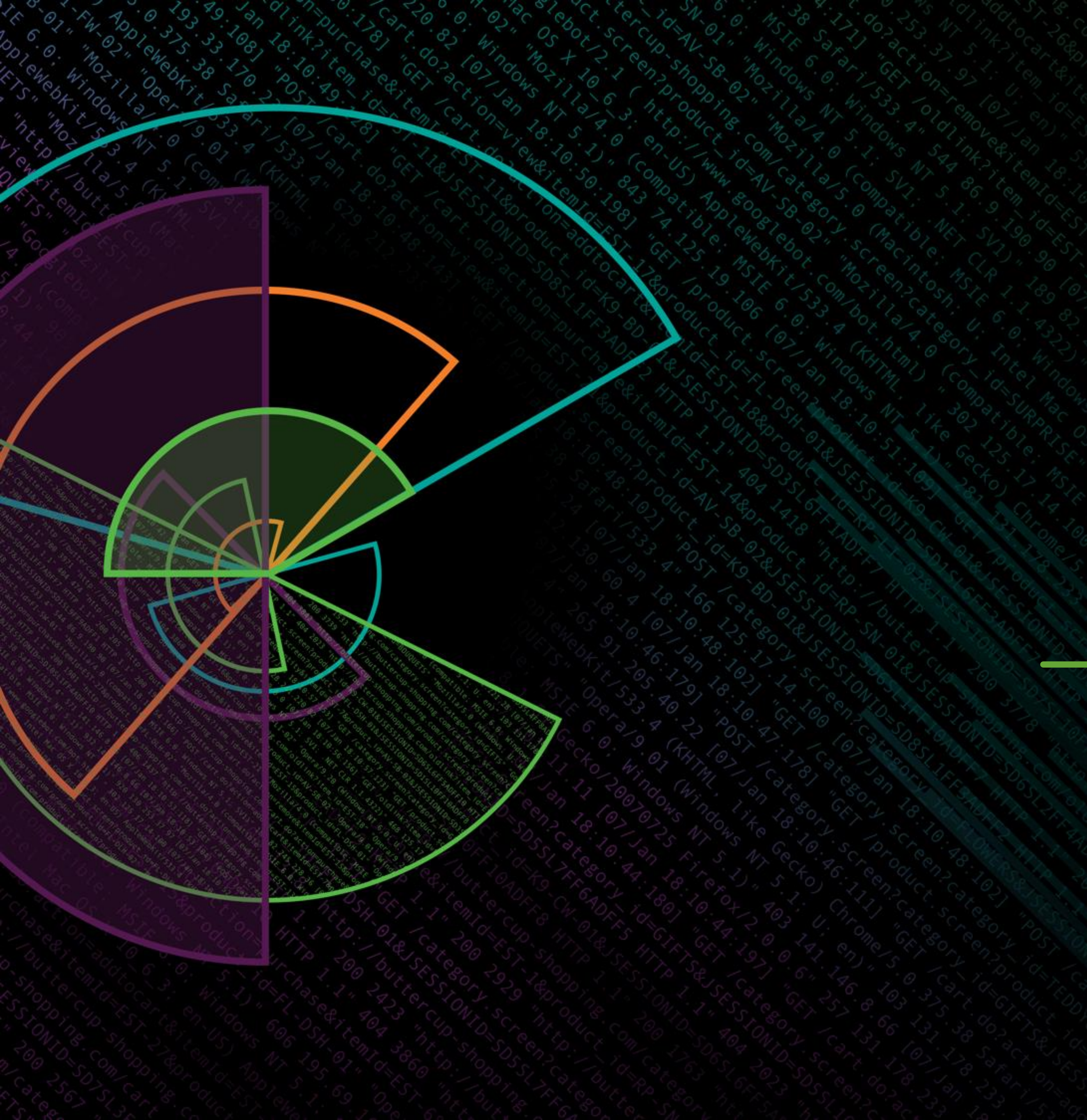
```
index=_internal sourcetype=splunkd source!="*/splunkforwarder/*" log_level=*
| stats count, count(eval(log_level=="ERROR")) AS error_count BY component
| where ( error_count / count ) > .5
```

✓ 117,829 events (8/27/18 10:58:55.000 AM to 8/27/18 11:13:55.000 AM)

component	count	error_count
CMSearchHead	1	1
ConfContentsCache	1	1
DistributedBundleReplicationManager	25	18
ExecProcessor	2042	1579
FrameworkUtils	21	21
GenerationGrabber	1	1
HttpClientRequest	1	1
KVStorageProvider	68	68

Result & Obvious Improvements

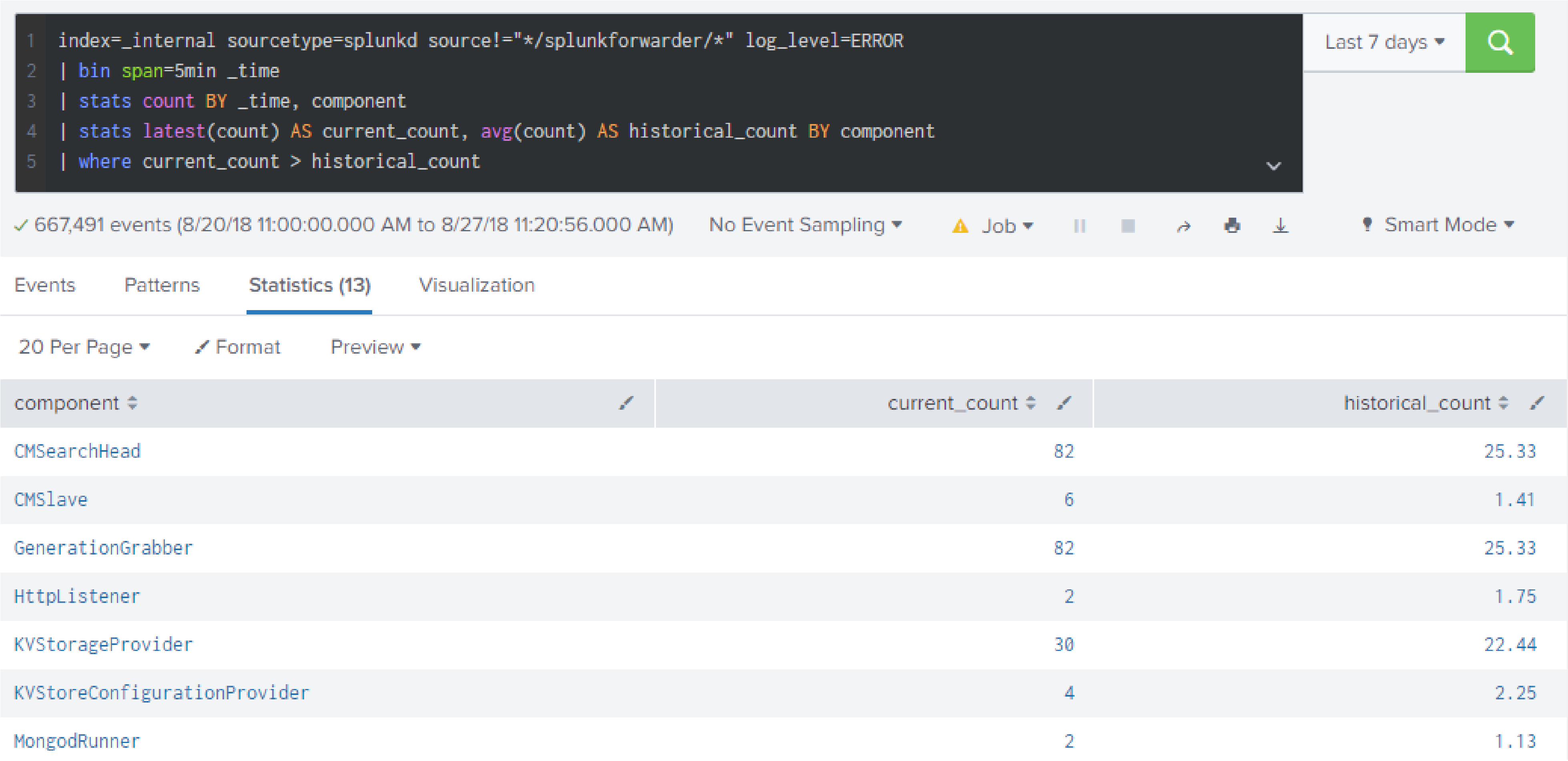
- Huge improvement
  - Less spam
  - Adjusts because normalized to volume
- What if that’s normal?
  - Then persistent alerts that should be ignored = spam + noise!
- Percentage => Static => Arbitrary?!



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
```

✓ 667,491 events (8/20/18 11:00:00.000 AM to 8/27/18 11:20:56.000 AM)

component	current_count	historical_count
CMSearchHead	82	25.33
CMSlave	6	1.41
GenerationGrabber	82	25.33
HttpListener	2	1.75
KVStorageProvider	30	22.44
KVStoreConfigurationProvider	4	2.25
MongodRunner	2	1.13

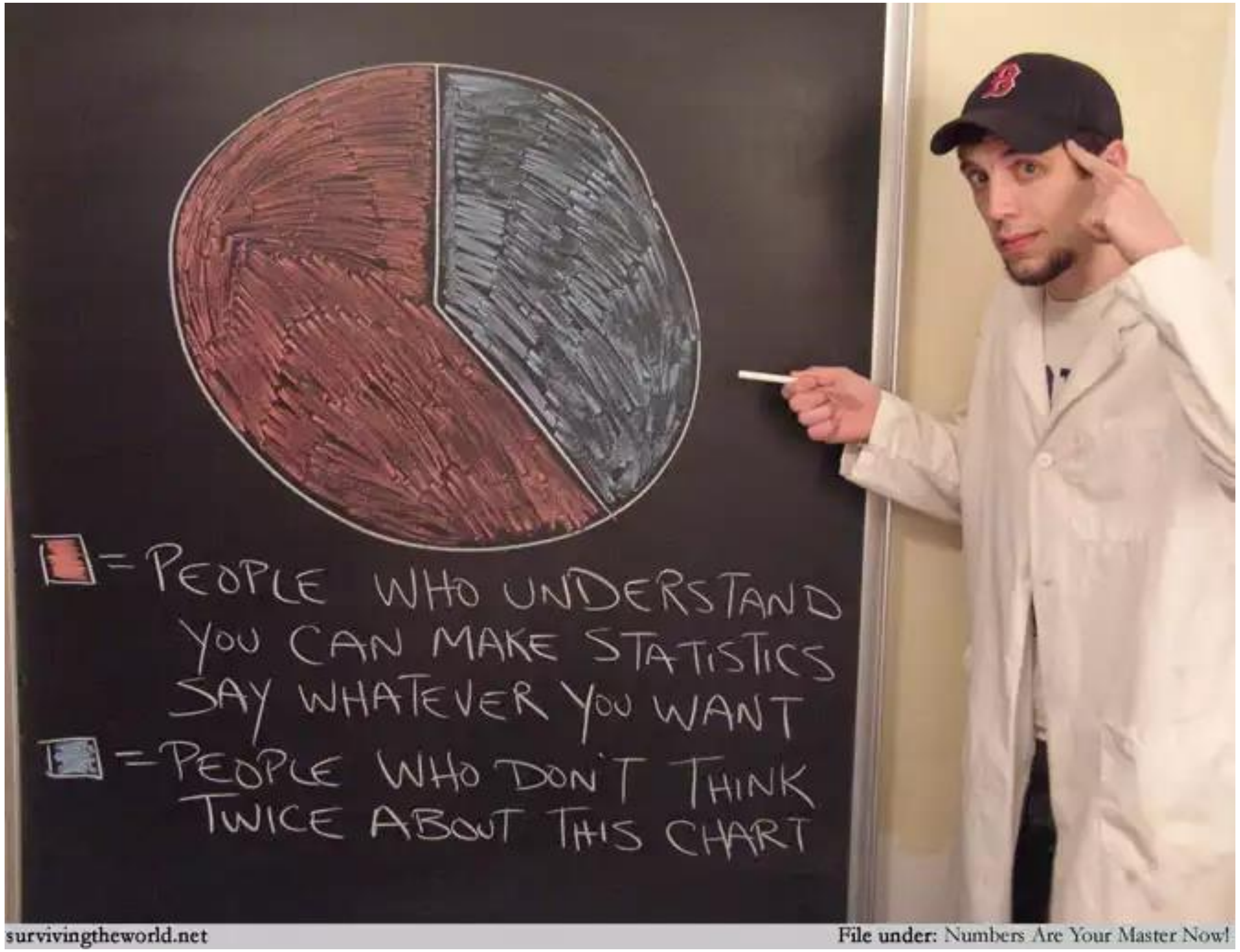
Result

- 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

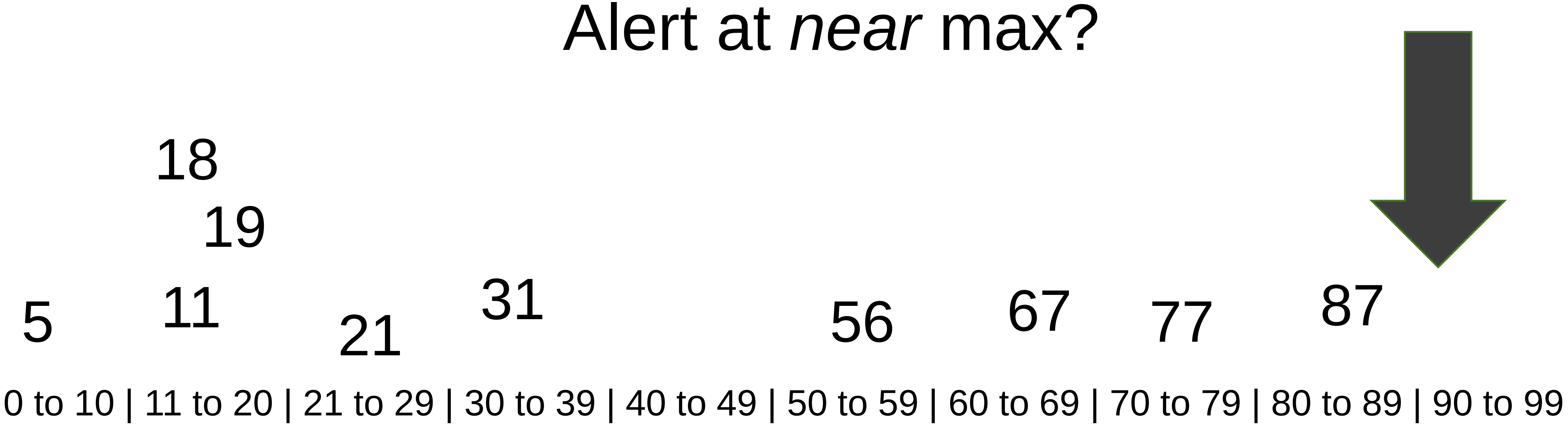
5 11 21 31 56 67 77 87

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

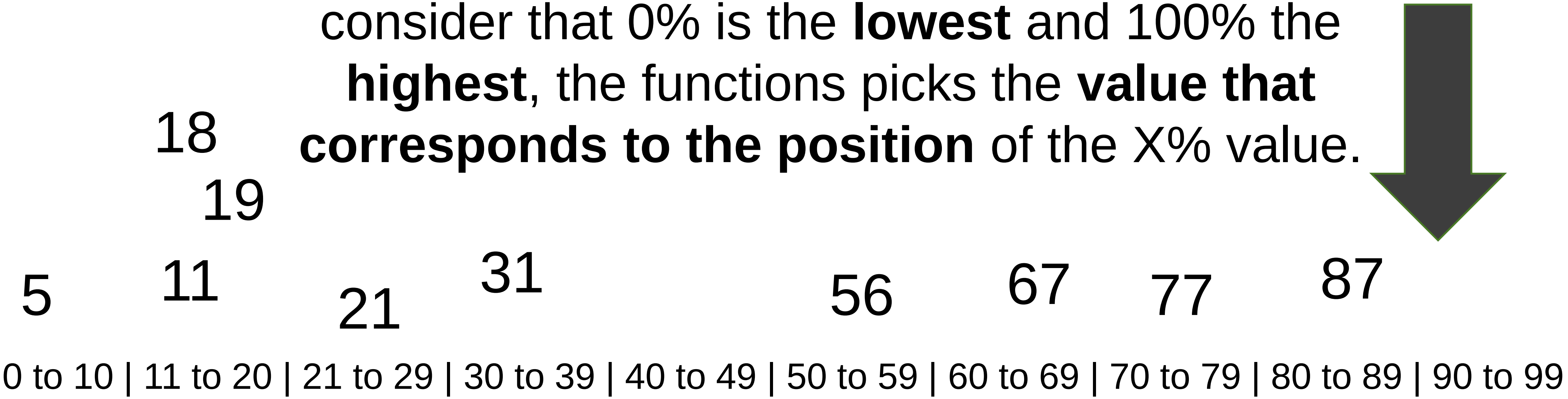
19

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

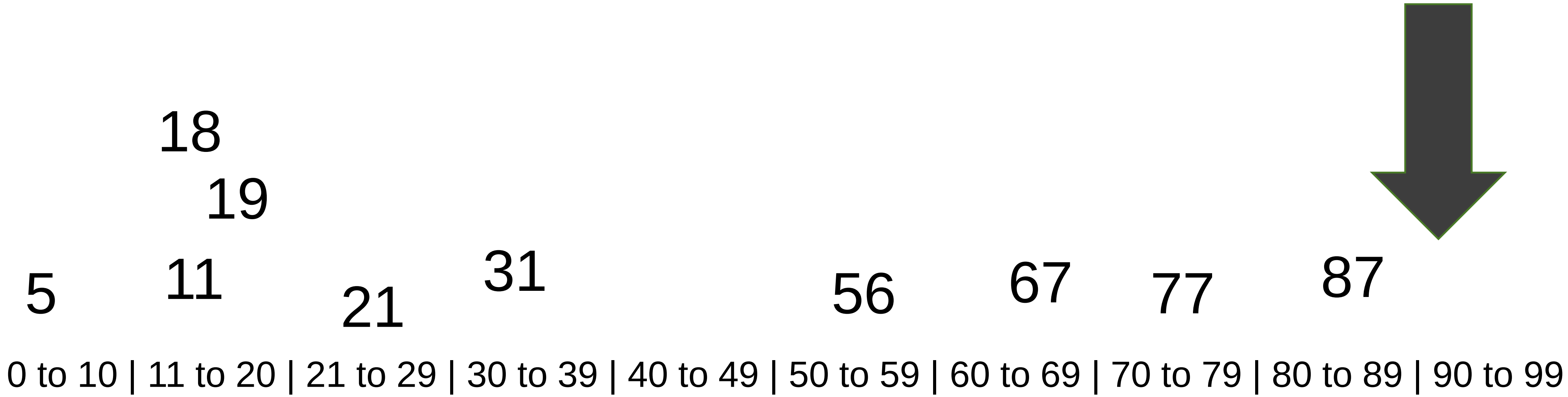
perc<X>(Y) = Returns the X-th percentile value of the numeric field Y, where X is an integer between 1 and 99. The percentile X-th function **sorts the values** of Y in an increasing order. Then, if you consider that 0% is the **lowest** and 100% the **highest**, the functions picks the **value that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



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

perc90(this_result_set) = ?



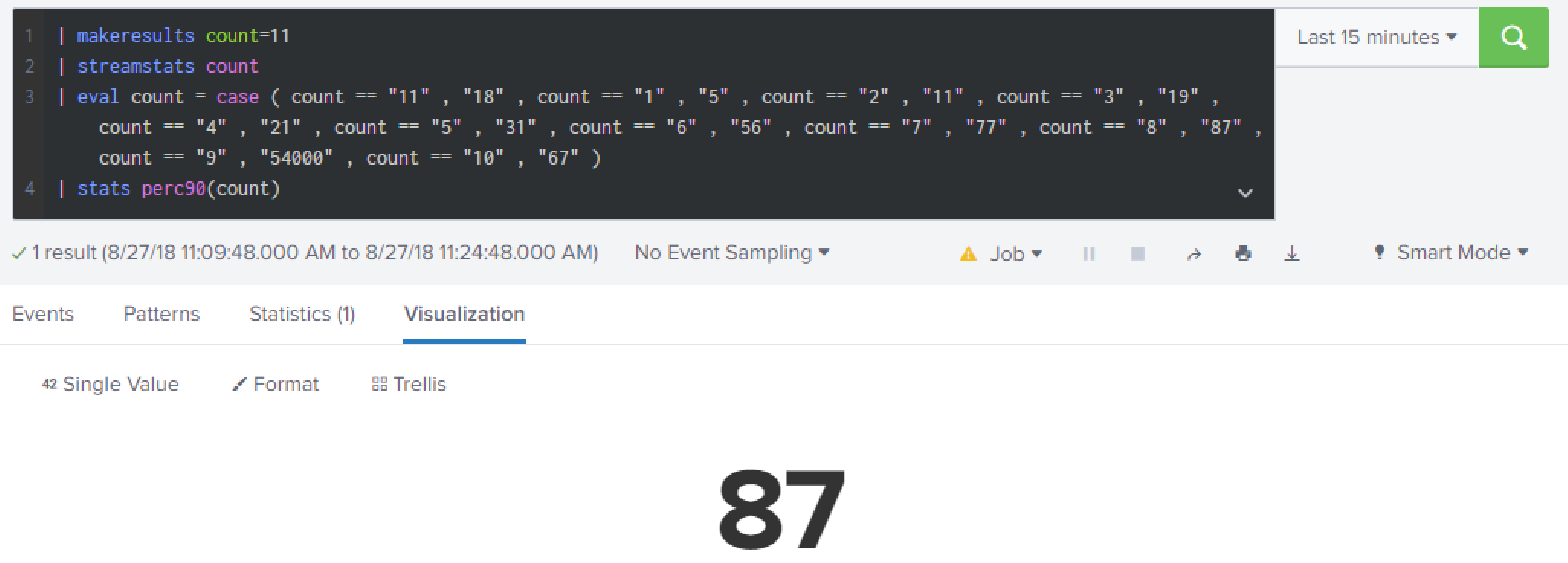
18

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 (8/27/18 11:09:48.000 AM to 8/27/18 11:24:48.000 AM)

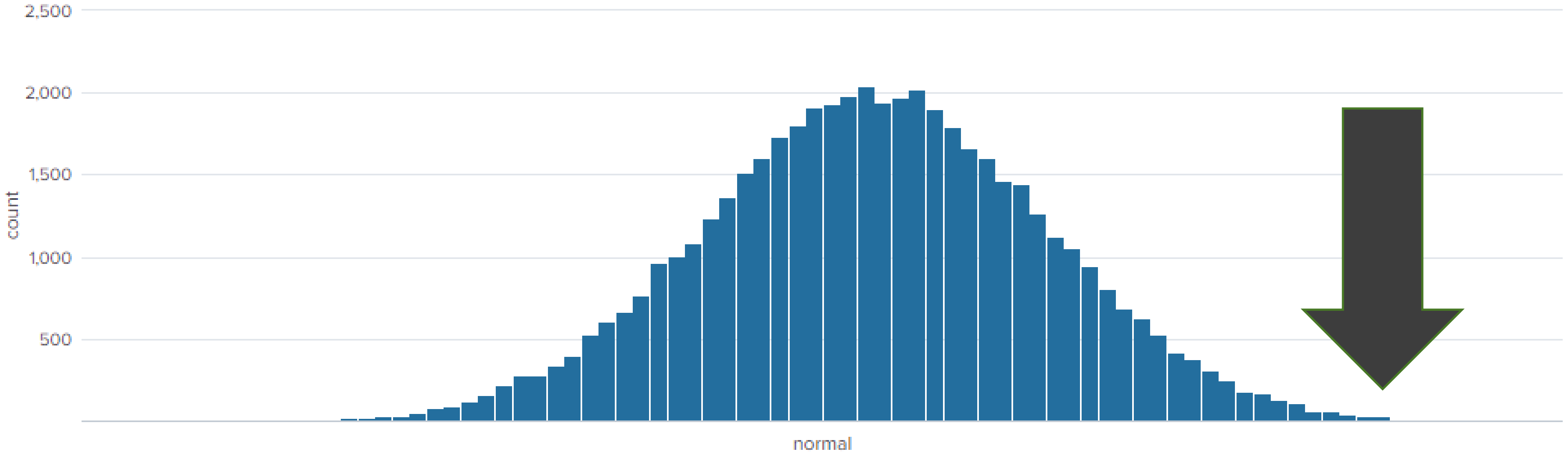
No Event Sampling ▾

Smart Mode ▾

87

Message > Thresholds > Relative % > **Averages** > Percentiles > ITSI > Actionable Alerts

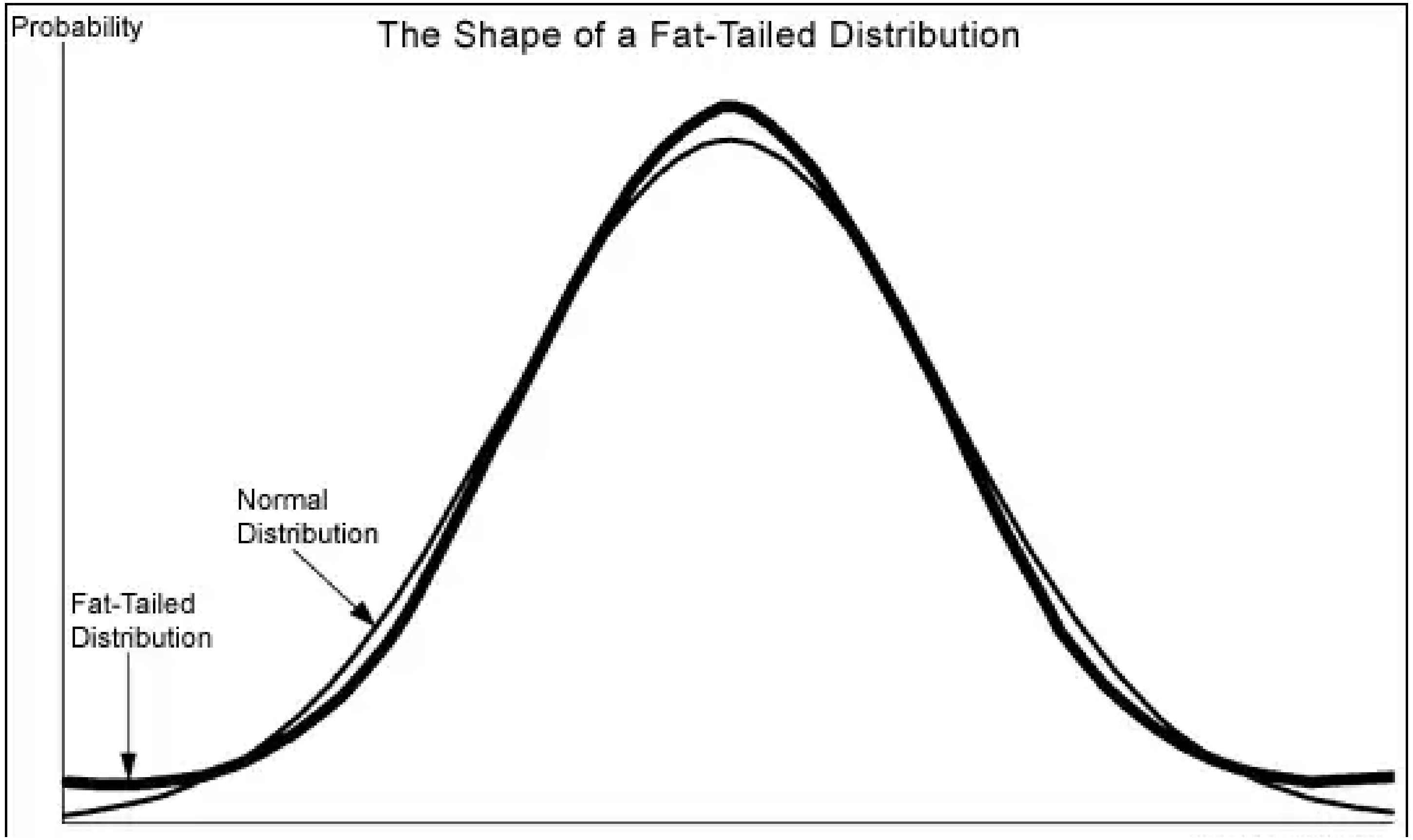
Warning: Assumption



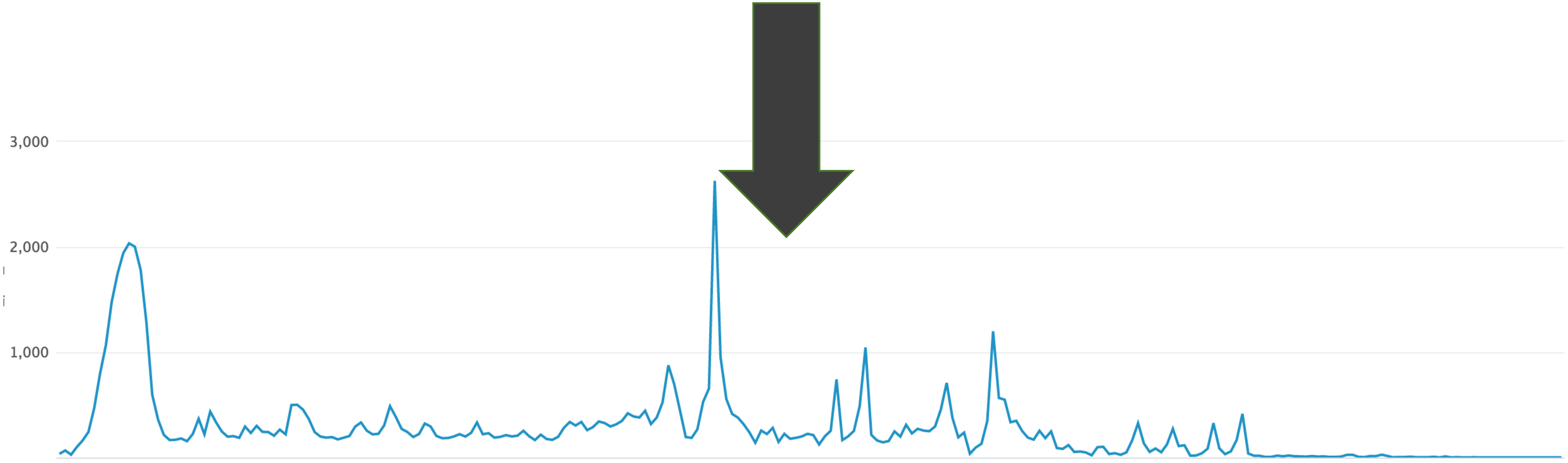
Shout out to Xander!

Message > Thresholds > Relative % > **Averages** > Percentiles > ITSI > Actionable Alerts

Warning: Heavy Tails

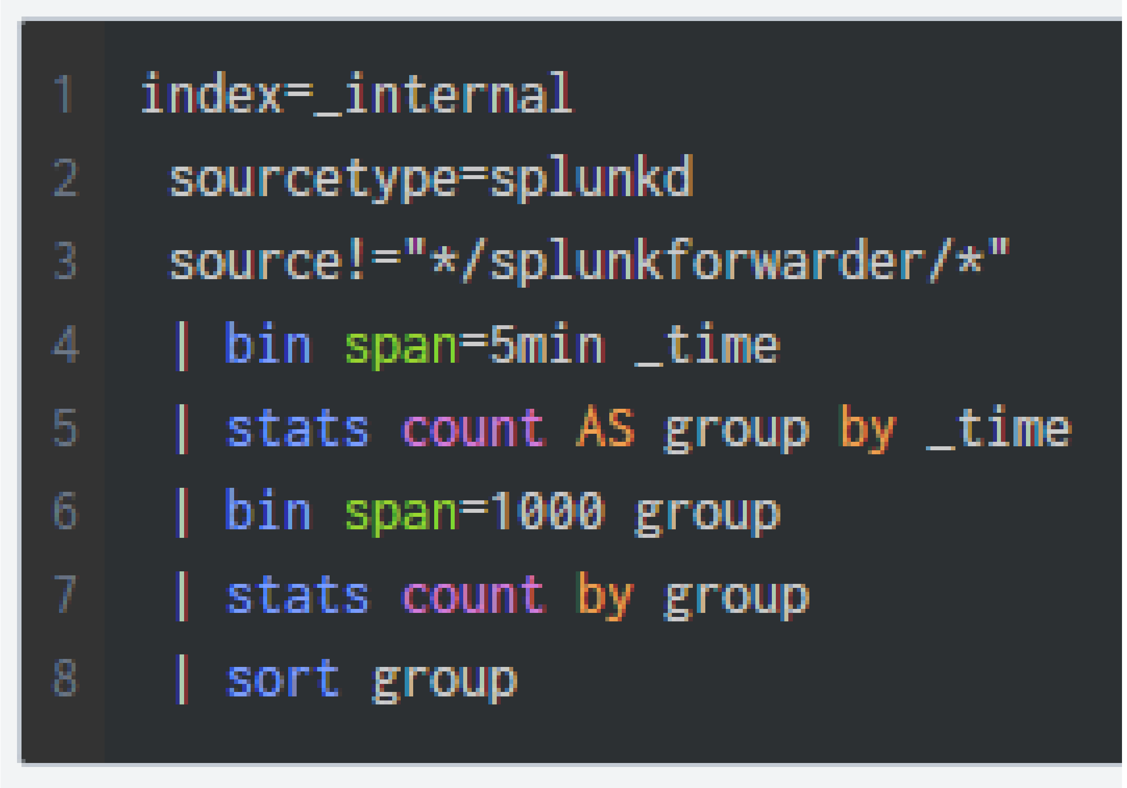


Warning: Reality

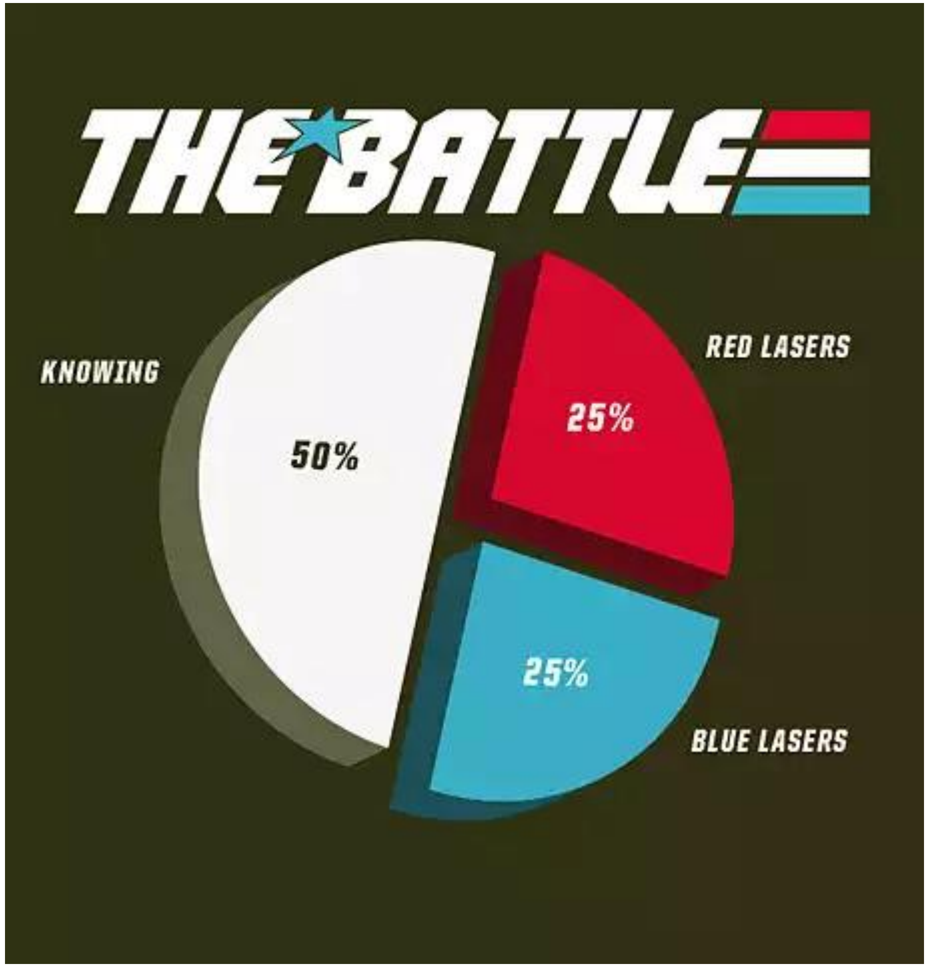


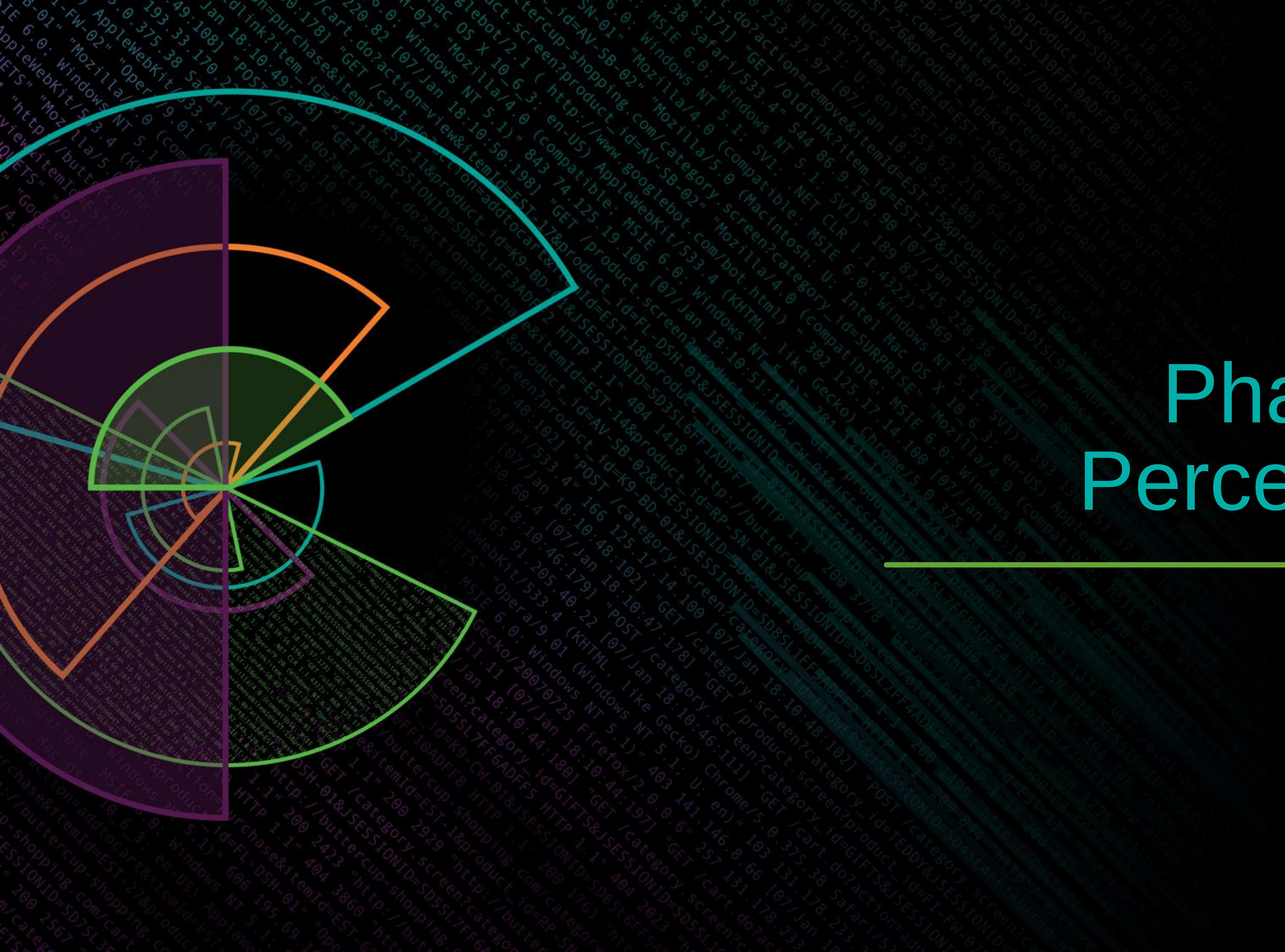
What percentile is appropriate given this distribution?

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
```

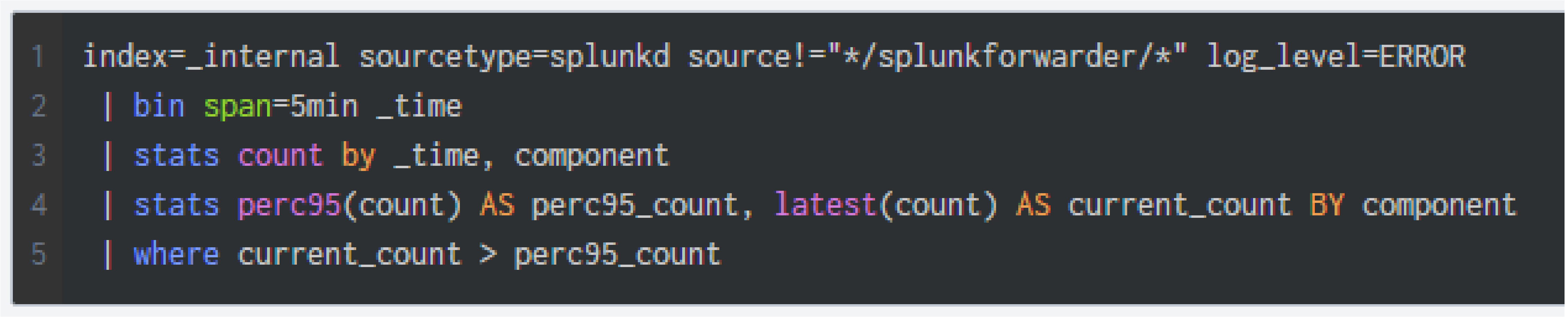




Phase 5: Percentiles

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?

The Lasso Approach

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

Message > Thresholds > Relative % > Averages > **Percentiles** > ITSI > Actionable Alerts

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

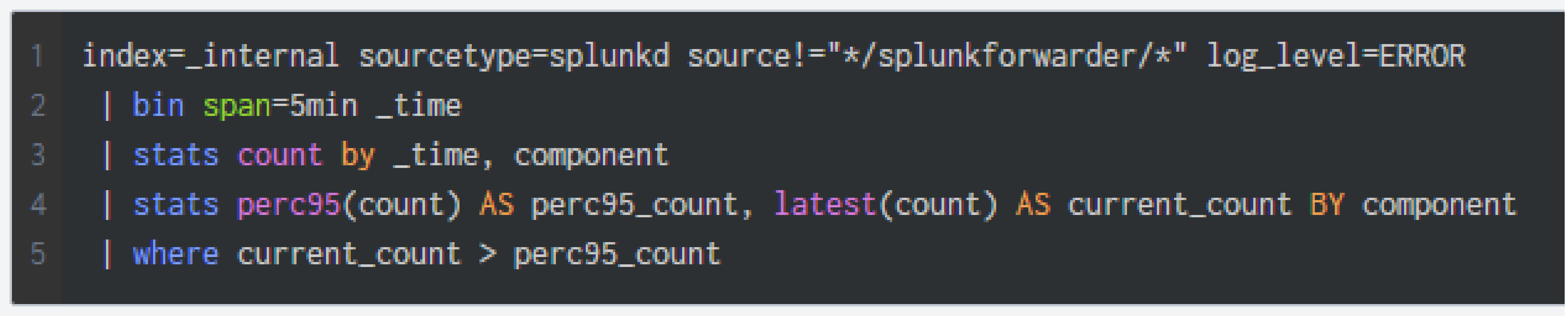
- Adjusts with changes in environment!

- Requires Maintenance
  - Power User skillz
  - Summary Indexing

- Not period time adjusted
  - Fluctuations in business day or period

Performance Detour

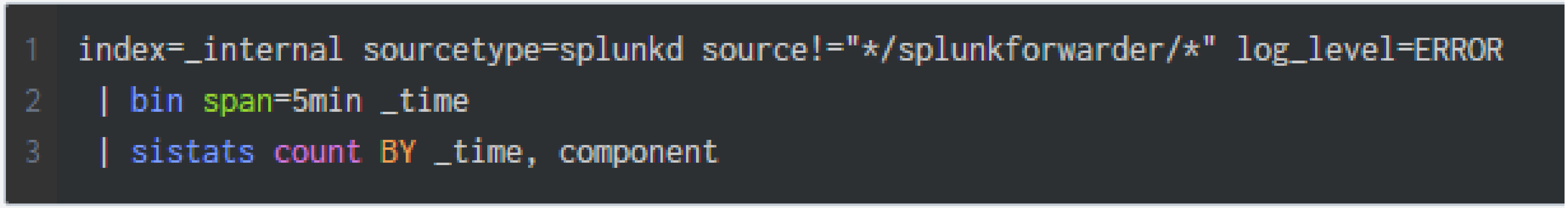
Massive Search



```
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
```

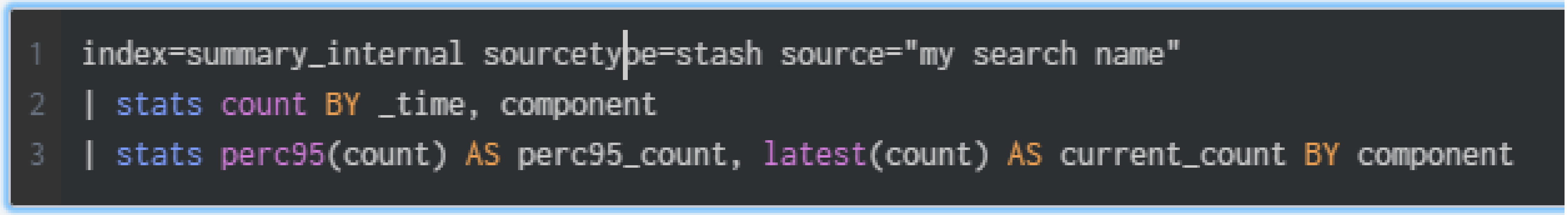
Summary Indexing Solution

- Generate malleable historical data (use snap-to times!)



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

- Alert upon historical data

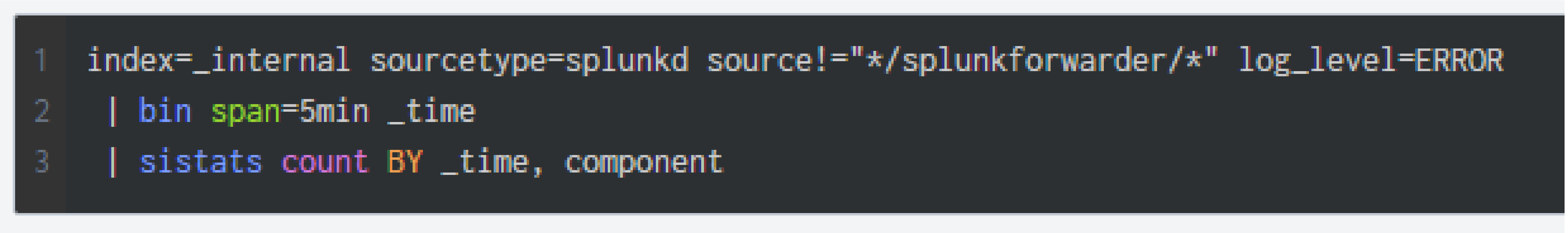


```
index=summary_internal sourcetype=stash source="my search name"
| stats count BY _time, component
| stats perc95(count) AS perc95_count, latest(count) AS current_count BY component
```

Develop with loadjob

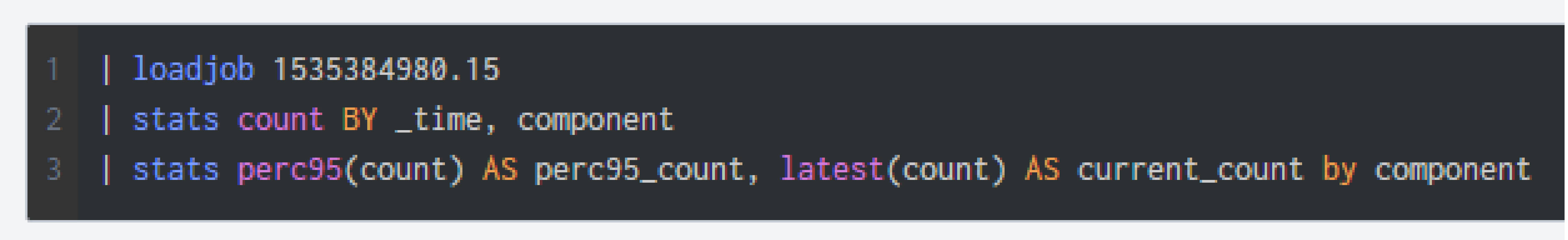
Caching!

- Generate result set



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

- Fetch result set to avoid re-searching



```
| loadjob 1535384980.15
| stats count BY _time, component
| stats perc95(count) AS perc95_count, latest(count) AS current_count by component
```

New Features

Logs as Metrics

gain performance > lose keyword search

Workload Management

control and prioritize the amount of system resources allocated

SmartStore

high volume data > caching implications

Search performance improvements

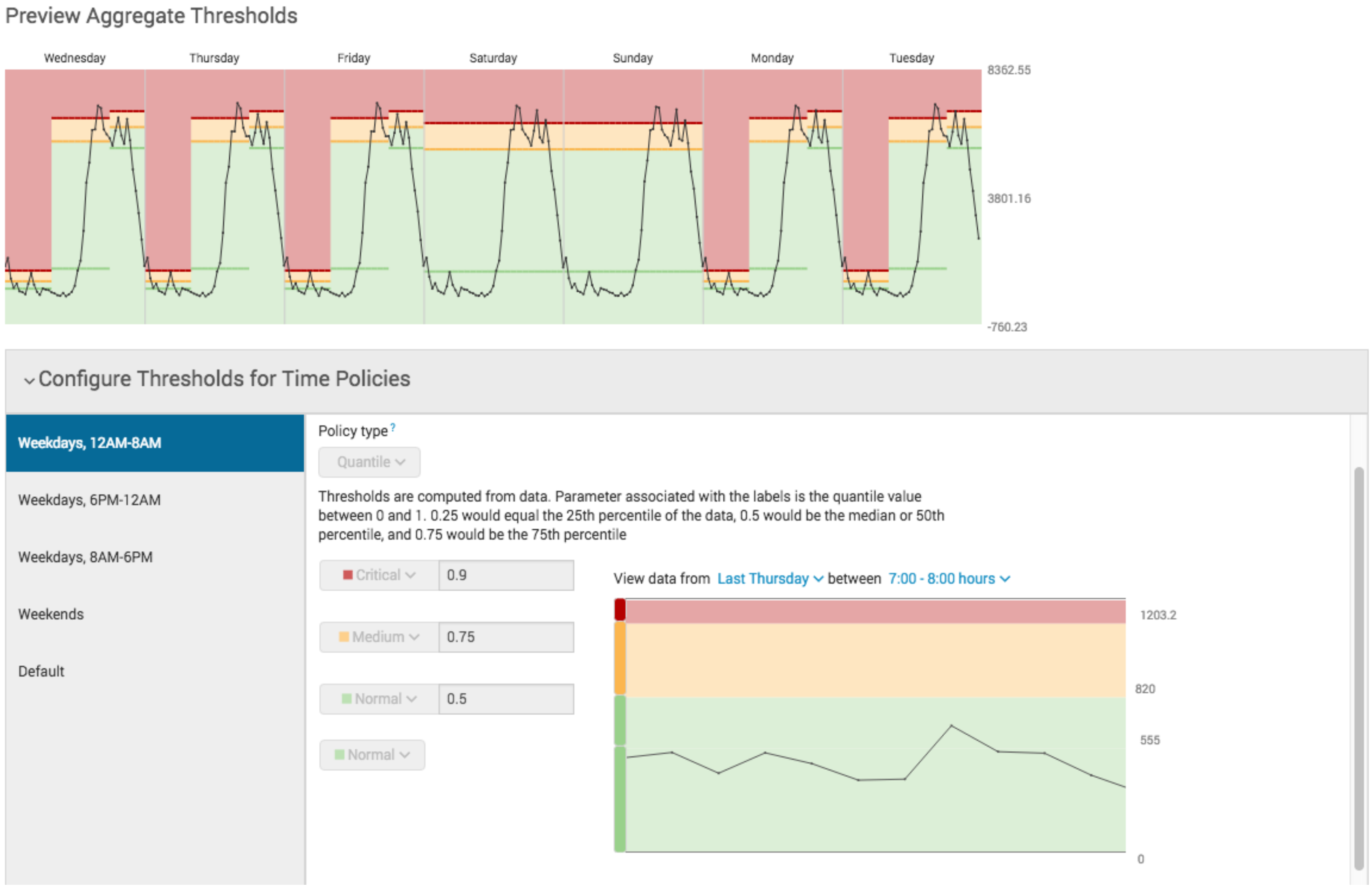
upgrade & enjoy

Bonus Phase 6: IT Service Intelligence

“Make actionable 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

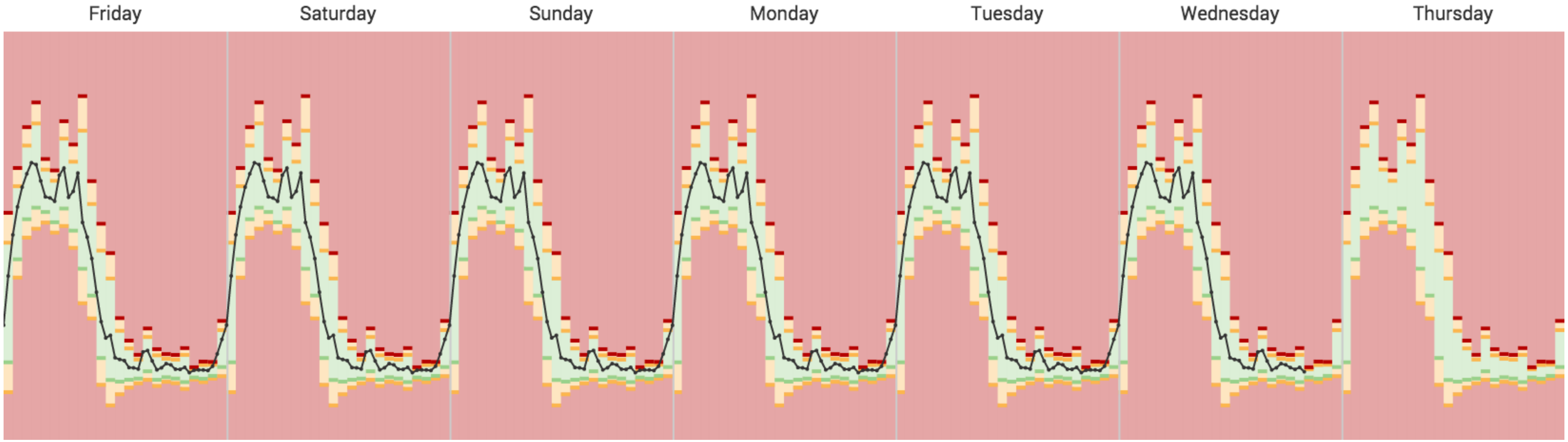
Thresholds are computed from data. Parameter associated with the labels is the quantile value between 0 and 1. 0.25 would equal the 25th percentile of the data, 0.5 would be the median or 50th percentile, and 0.75 would be the 75th percentile

🟥 Critical	0.9
🟧 Medium	0.75
🟩 Normal	0.5
🟩 Normal	

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

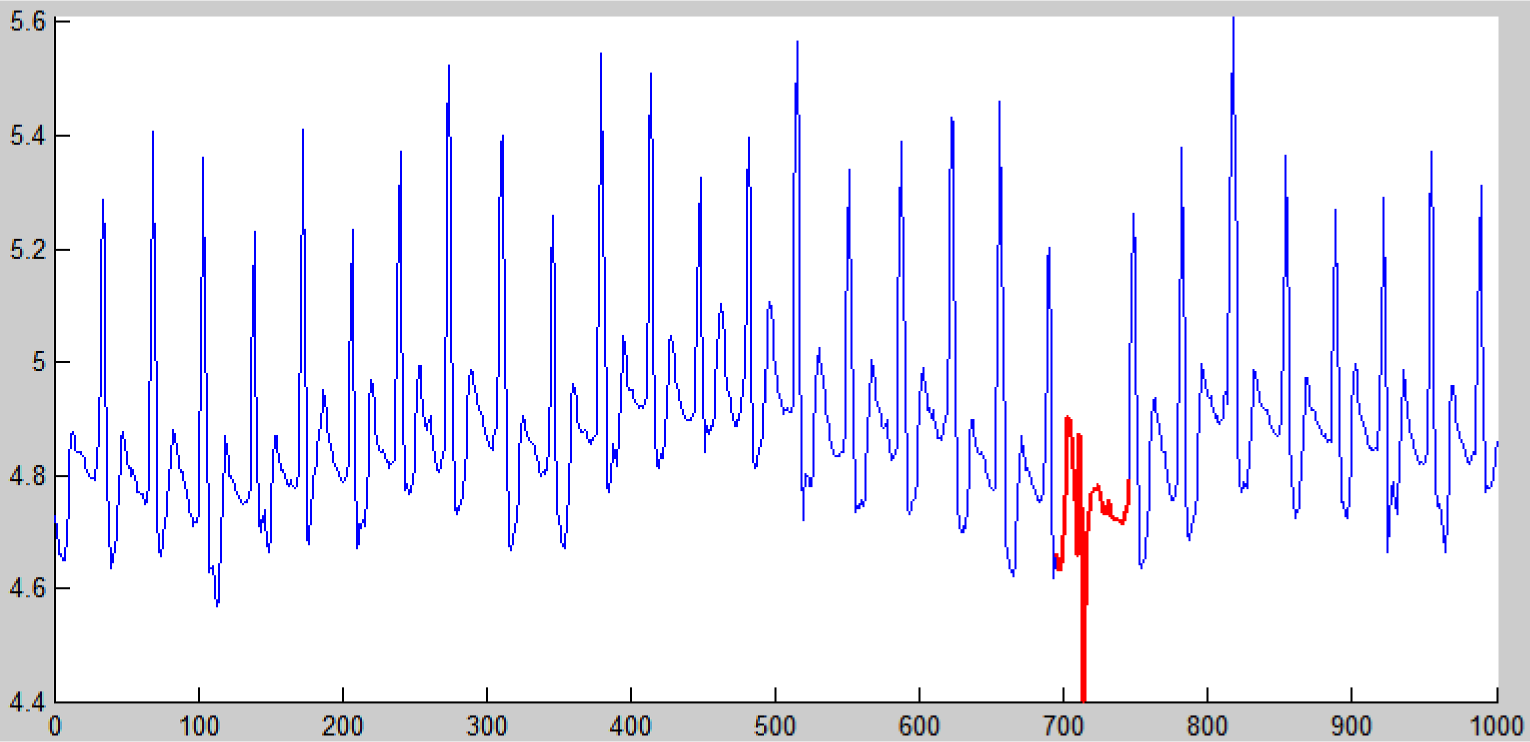
Message > Thresholds > Relative % > Averages > Percentiles > **ITSI** > Actionable Alerts

Adaptive Thresholds

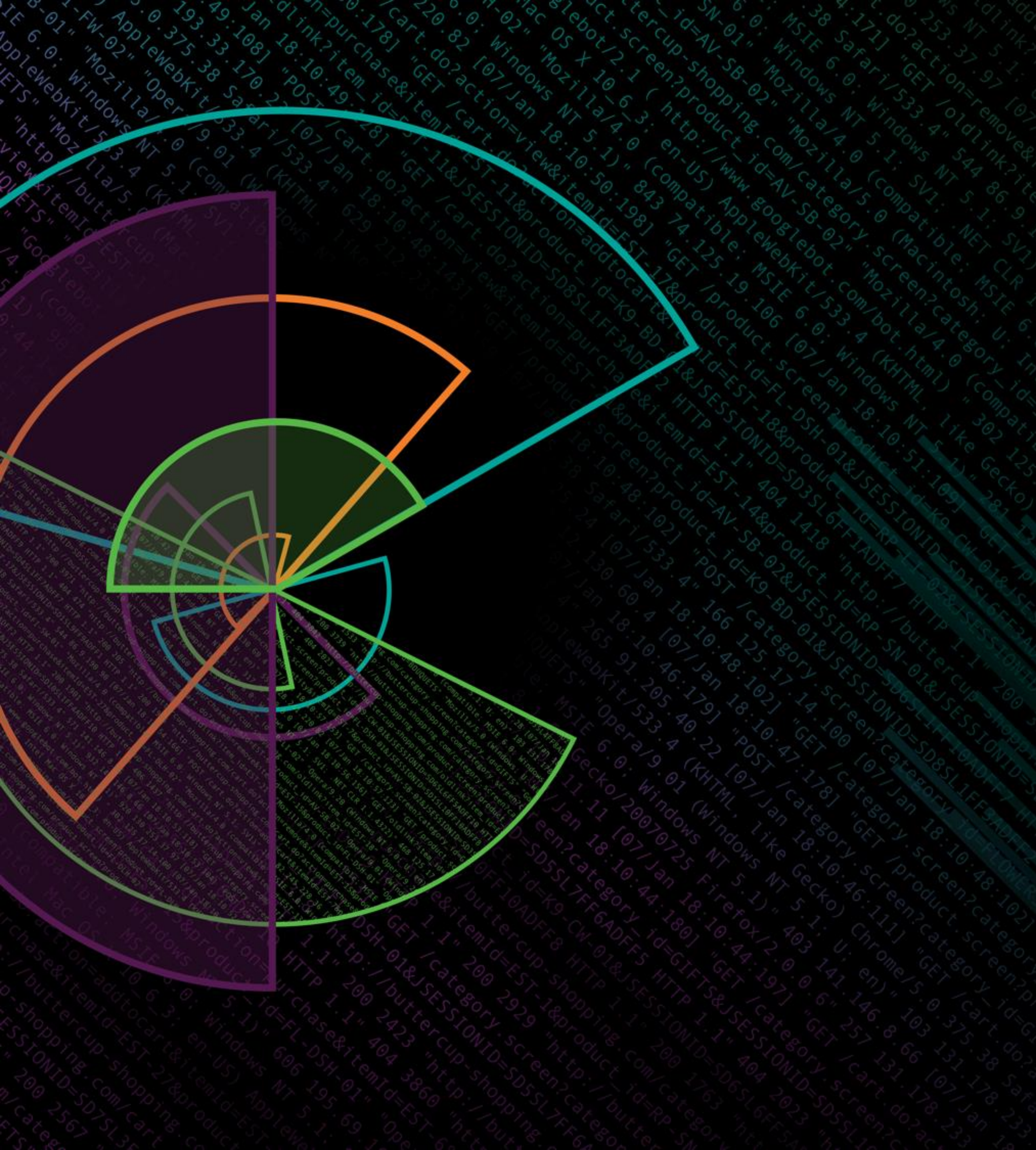


Message > Thresholds > Relative % > Averages > Percentiles > **ITSI** > Actionable Alerts

Anomaly Detection



Message > Thresholds > Relative % > Averages > Percentiles > **ITSI** > Actionable Alerts



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…

1. Rate this! (be honest)
2. Collaborate: #alerting
   - Sign Up @ http://splk.it/slack
3. More talks, search for
   - Burch
   - Jeff Champagne
   - Delaney
   - Stefan
   - Veuve

Questions & Discussion?

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

.conf18

splunk>