Alerting in grafana

Dieter Plaetinck

Grafanacon 2015 NYC

Dieter Who?

- Graph-Explorer, metrics 2.0
- graphite-ng, carbon-relay-ng
- anthracite
- graphite-influxdb, influx-cli, whisper-to-influxdb
- Bosun ~ graphite
- http://dieter.plaetinck.be/tags/monitoring/

quixotic

quix · ot · ic

/kwik'södik/

adj

Idealistic without regard to practicality.

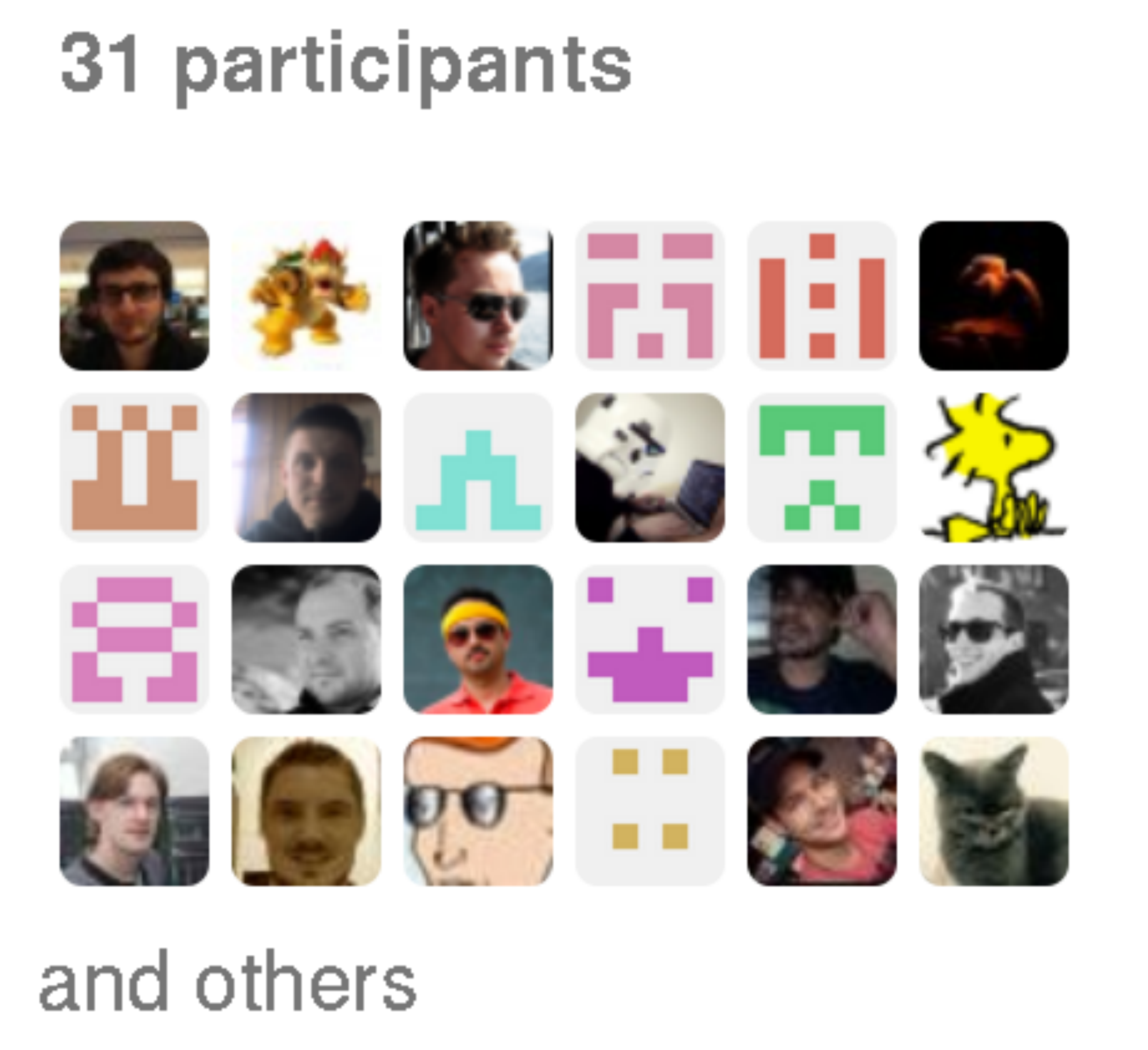
raintank

♥

Grafana

Re-arranging
Sparklines
SpeedOmeter
Synchronizing
Classifier
Theming
Timeshift
images
metadata
scripting
Y-axis.
widgets
InfluxDB
discovery
Plugins
Thresholds
user
Direct
Multi-tenancy
Nodes
reactions
raspberry
tags
Repository
Templating
LDAP
events
AWS
Alerting
Export/Share
Solr
Authentication
Linking
layouts
KairosDB
Support
db
3D
Integrated
Lightweight
scrolling
Cloudwatch
Backend
heatmaps
More Charts
Panels
Sensu
reports
data sources
perfmon
re-plot
Pie
Customization
controls
community
tree-based
permalinks
Legend
permissions/roles
OpenTSDB
annotations
Integration
Cache
Time
History
notifications
language
Banana
Maps
snoopad
team
Variables
HierarchyBar
Kibana
SQL
API
playlists
background
printing
Histograms
timerange
disk
websocket
Public
Riemann
pulling
snmp
standalone
Puppet
importing
Logarithmic

Anthony • Dieter • Matt • Raj • Torkel



31 participants

and others

https://github.com/grafana/grafana/issues/2209

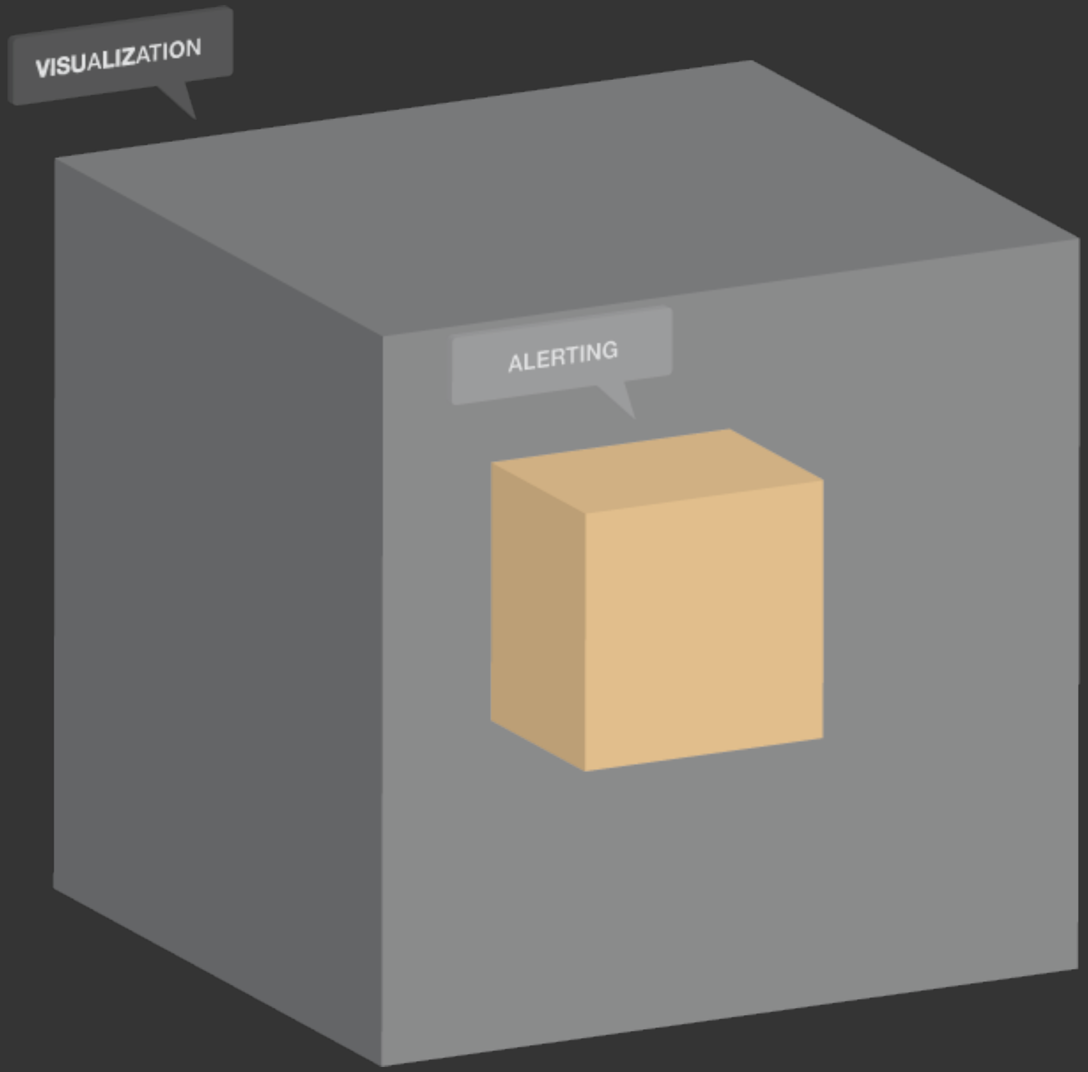
Idealized
design

http://www.ida.liu.se/~steho87/und/htdd01/AckoffGuidetoIdealizedRedesign.pdf

http://knowledge.wharton.upenn.edu/article/idealized-design-how-bell-labs-imagined-and-created-the-telephone-system-of-the-future/

brainstorm

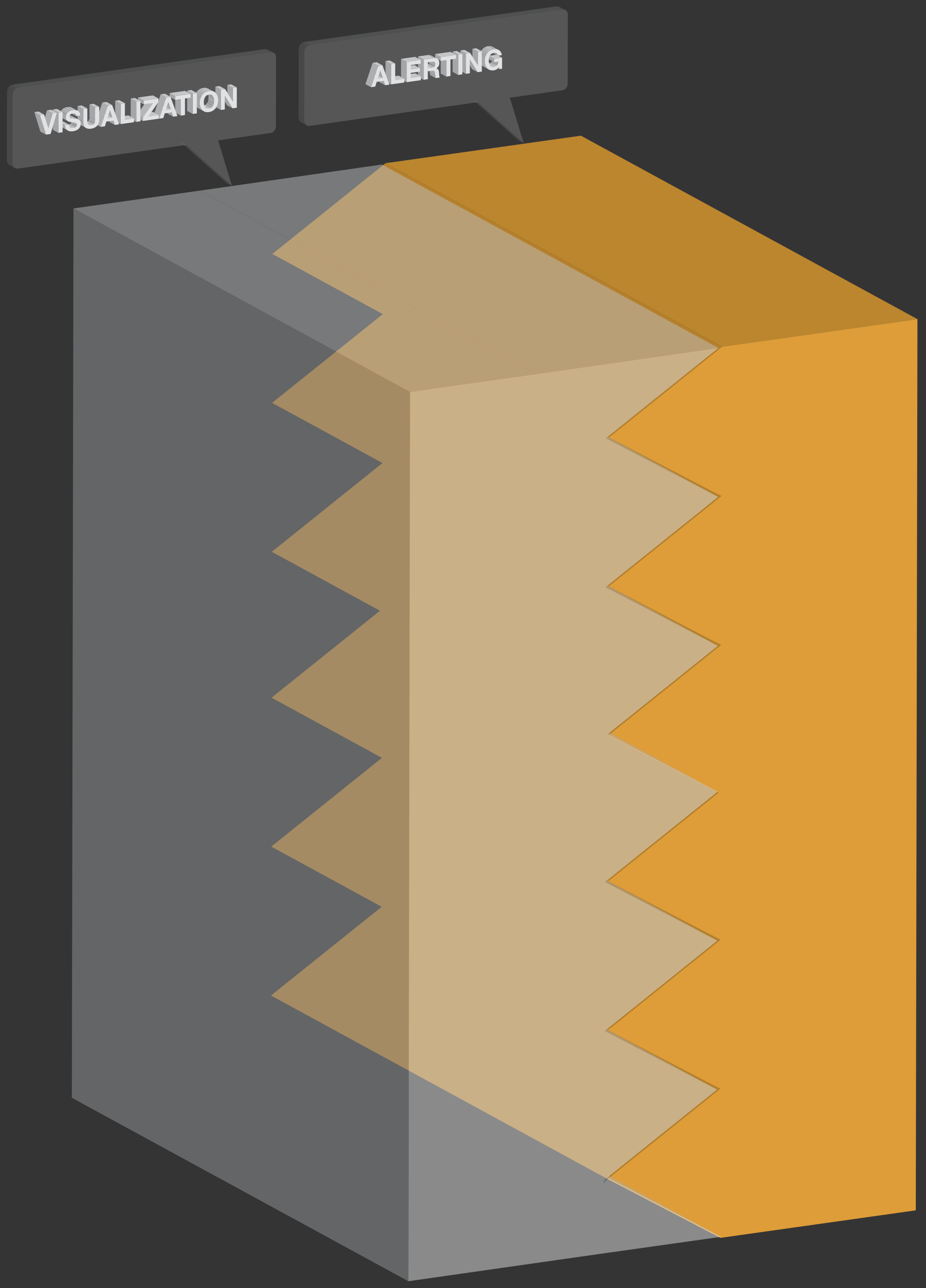
Scope of alerting



Scope of alerting

VISUALIZATION
ALERTING

Scope of alerting



UX

driven

second
system
syndrome

saying no.

Learning from Grafana

Prevent people from doing stupid things

Prevent people from doing stupid things

Prevent people from doing smart things

Focus

on

power users

Finding the balance on a small budget

really

really

really

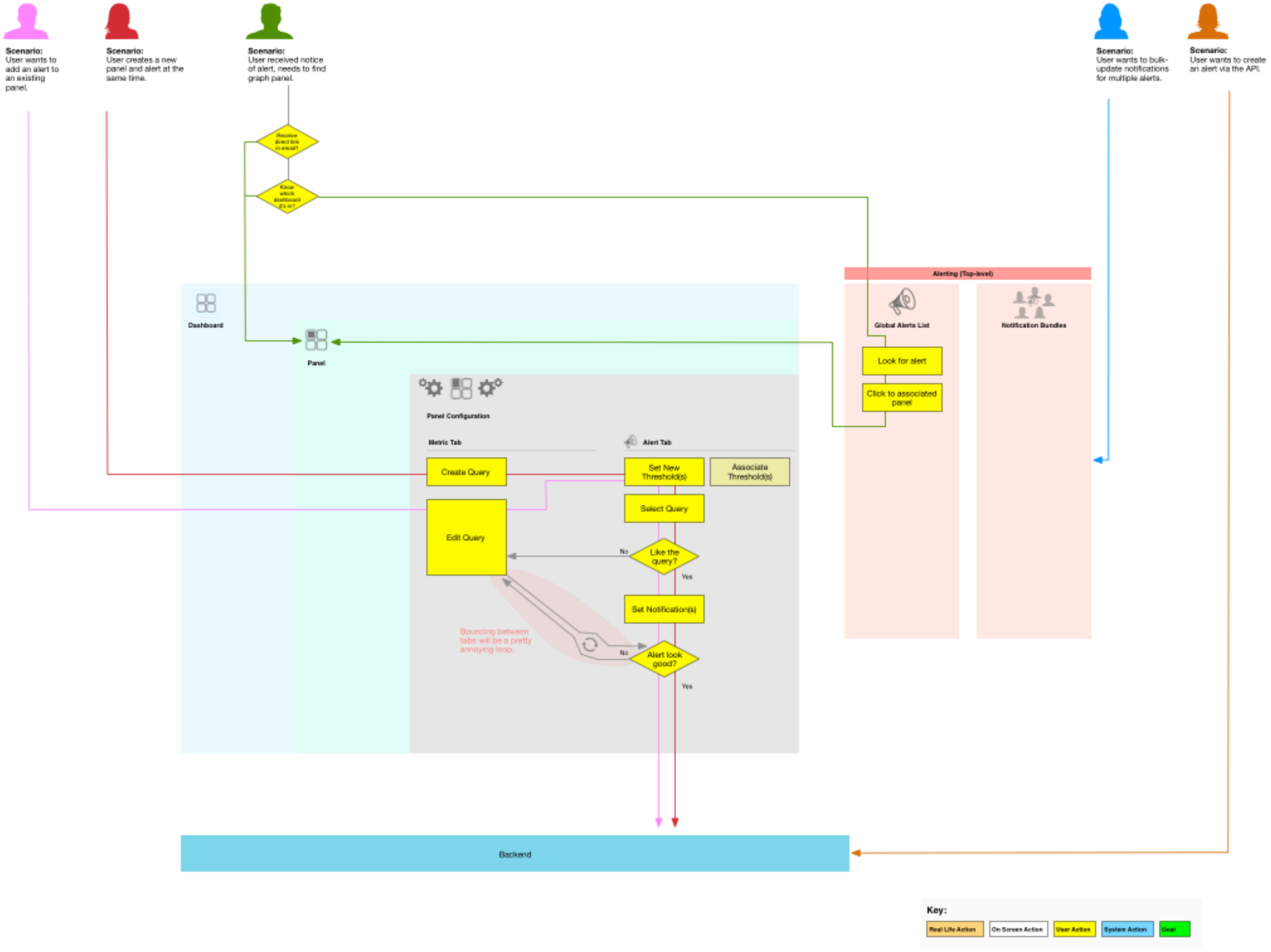
HARD

prototype

iterate

evolvable design

user workflow



Scenario: User wants to add an alert to an existing panel.

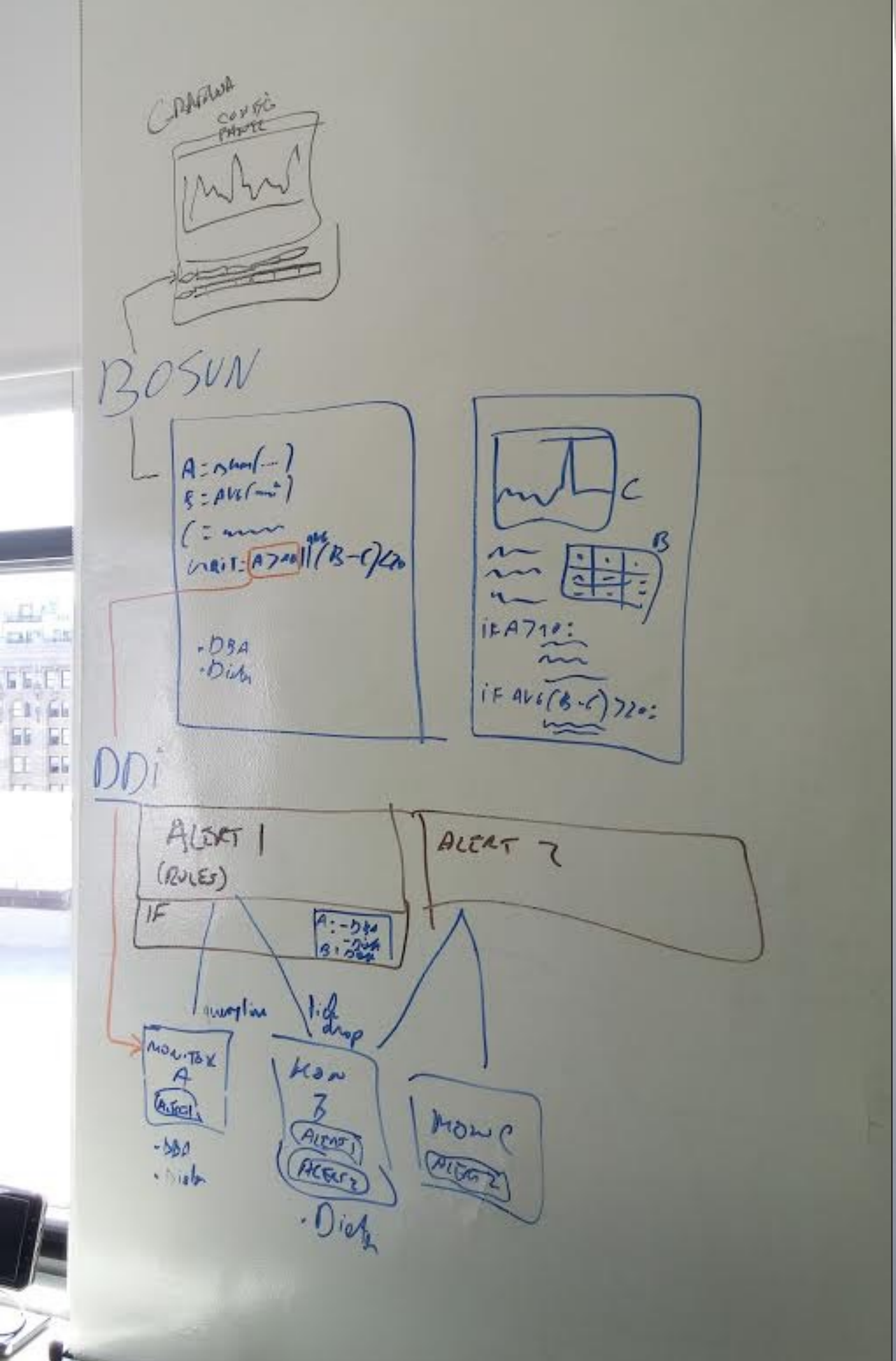
Scenario: User creates a new panel and alert at the same time.

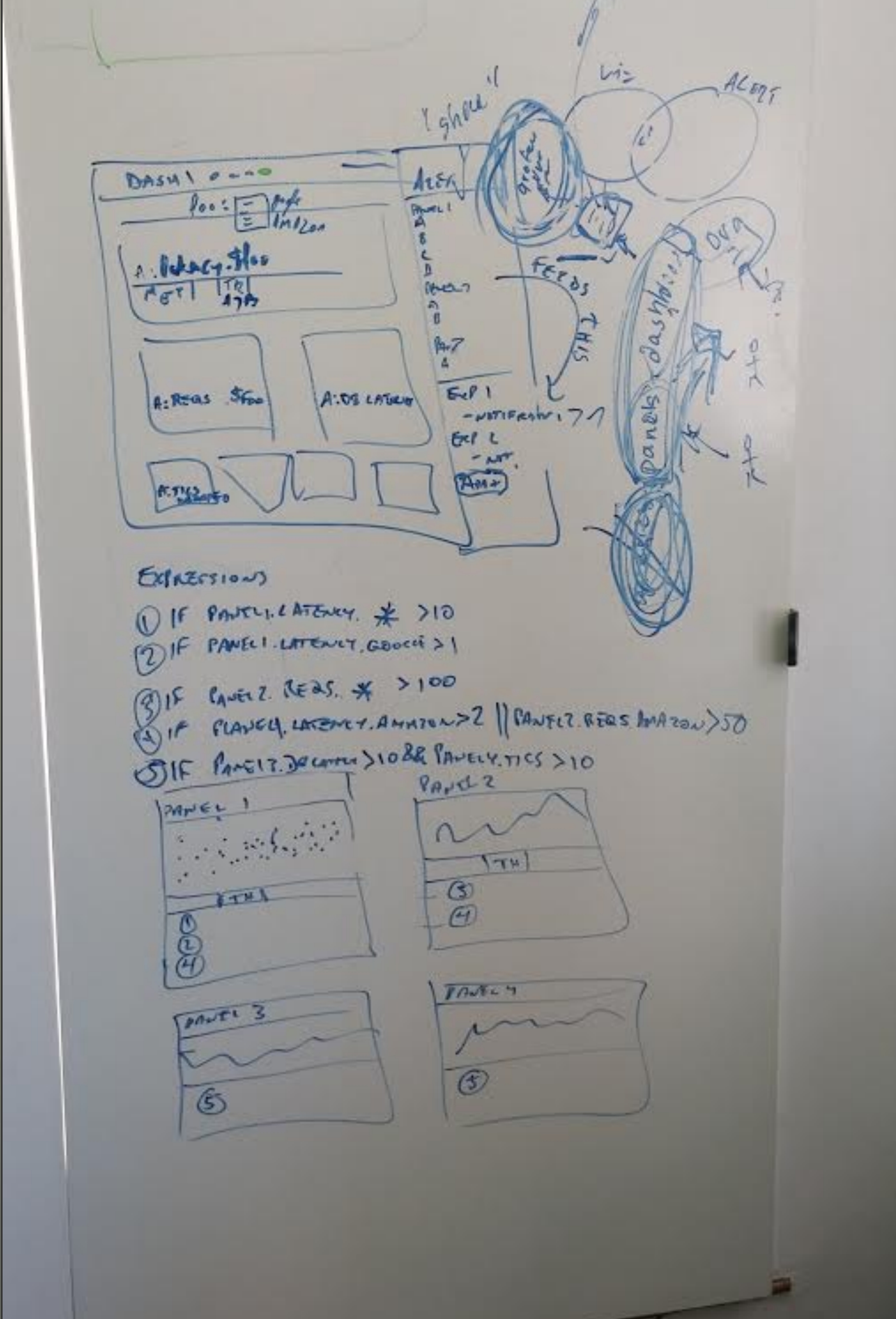
Scenario: User received notice of alert, needs to find graph panel.

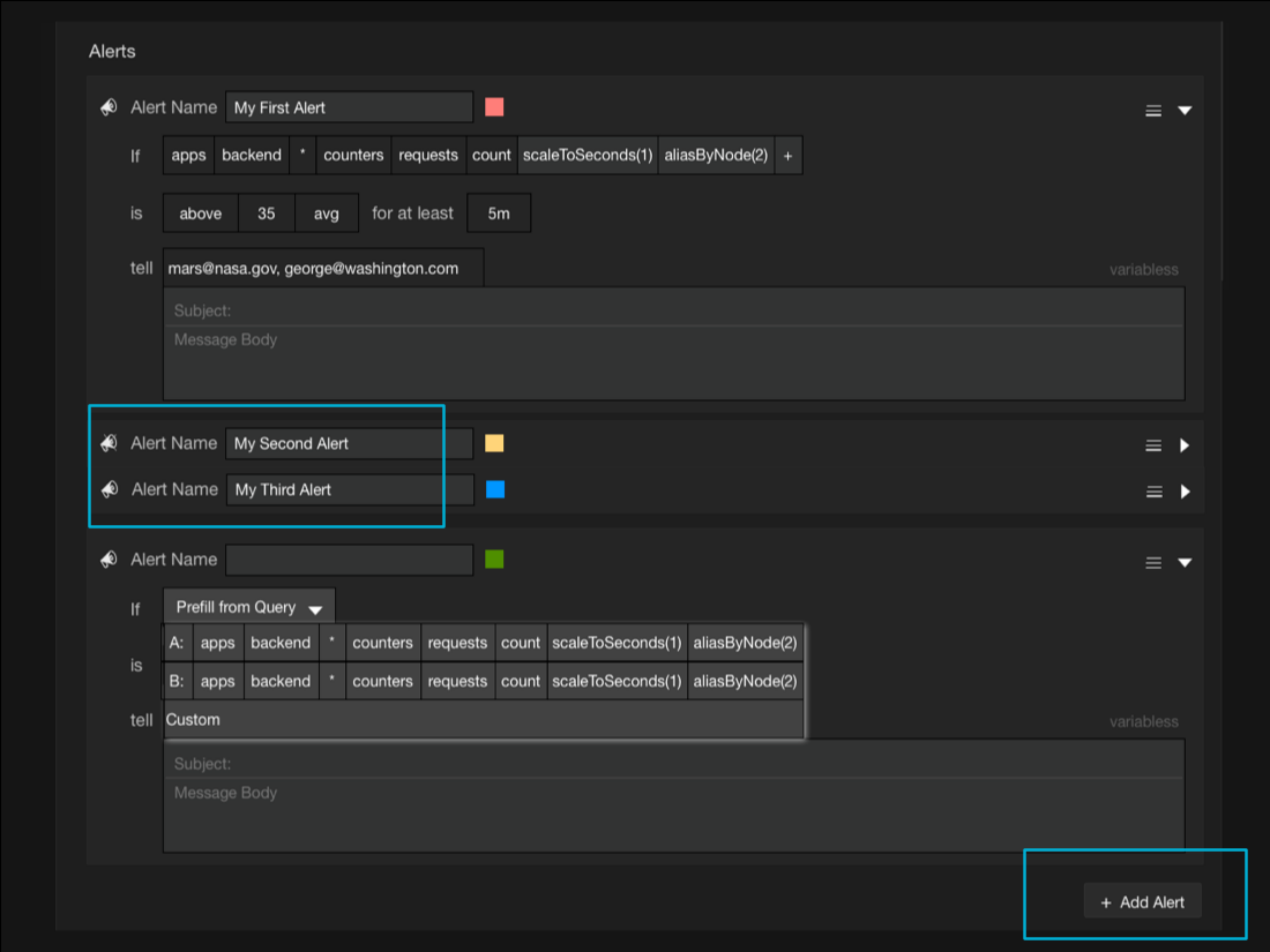
Scenario: User wants to bulk-update notifications for multiple alerts.

Scenario: User wants to create an alert via the API.

mockups!


GRAFANA
CONFIG PANEL
BOSUN
A = ...
B = AVG(...)
C = ...
CRIT: A>10 || (B-C)<20
· DBA
· Dick
C
B
IF A>10:
IF AVG(B-C)>20:
DDi
ALERT 1
(RULES)
IF
A: - DBA
B: - DBA
ALERT 2
MONITOR A
ALERT 1
· DBA
· Dick
MON B
ALERT 1
ALERT 2
· Dick
MON C
ALERT 2


DASH 1
foo:
AMAZON
A: LATENCY. $foo
MET
TH
A: REQS $foo
A: DB LATENCY
A: TICS $foo
ALERT
PANEL 1
A
B
C
D
PANEL 2
A
B
PANEL 3
A
EXP 1
- NOTIFICATION
EXP 2
- NOT.
FEEDS THIS
VIZ
ALERT
dashboards
panels
EXPRESSIONS
① IF PANEL1.LATENCY. * >10
② IF PANEL1.LATENCY.GOOGLE >1
③ IF PANEL2.REQS. * >100
④ IF PANEL4.LATENCY.AMAZON>2 || PANEL2.REQS.AMAZON>50
⑤ IF PANEL3.DB LATENCY>10 && PANEL4.TICS >10
PANEL 1
TH
①
②
④
PANEL 2
TH
③
④
PANEL 3
⑤
PANEL 4
⑤



Alerts

Alert Name My First Alert

If apps backend * counters requests count scaleToSeconds(1) aliasByNode(2)

is above 35 avg for at least 5m

tell mars@nasa.gov, george@washington.com

Alert Name My Second Alert

Alert Name My Third Alert

Alert Name

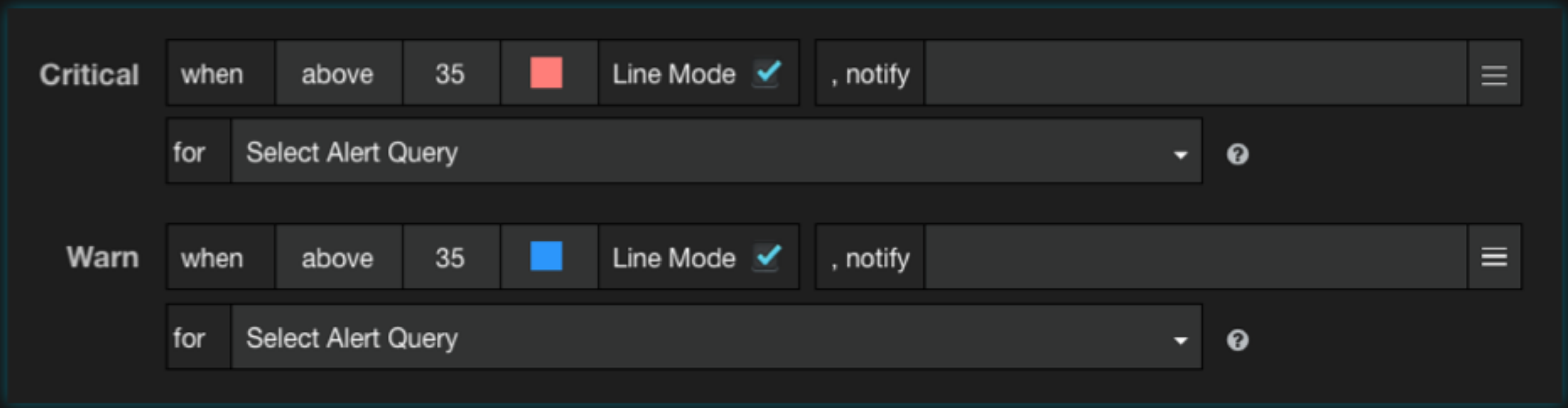
If

A: apps backend * counters requests count scaleToSeconds(1) aliasByNode(2)

B: apps backend * counters requests count scaleToSeconds(1) aliasByNode(2)

is

tell Custom

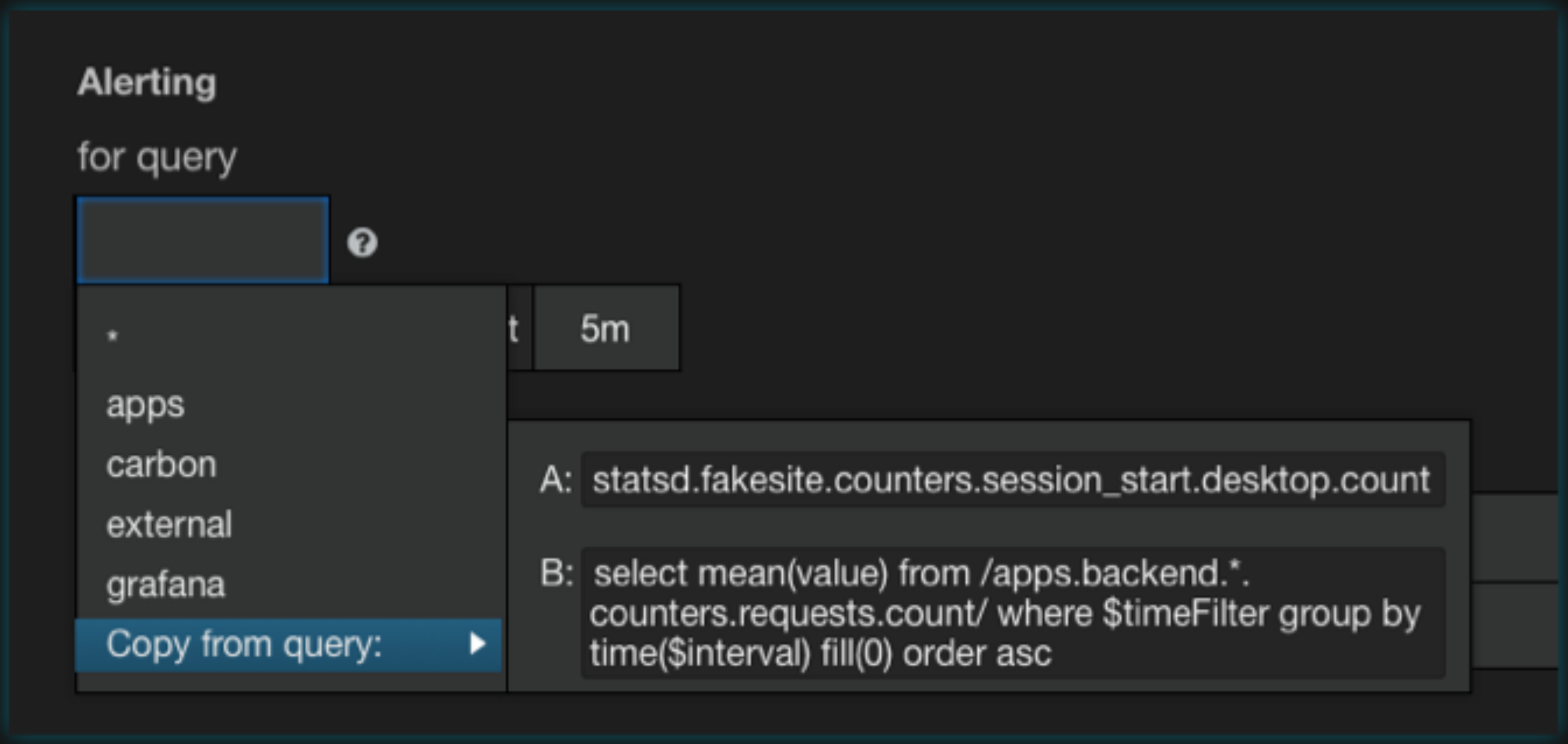


Critical | when | above | 35 | 🟥 | Line Mode ✓ | , notify | ☰

for | Select Alert Query ▾ | ?

Warn | when | above | 35 | 🟦 | Line Mode ✓ | , notify | ☰

for | Select Alert Query ▾ | ?

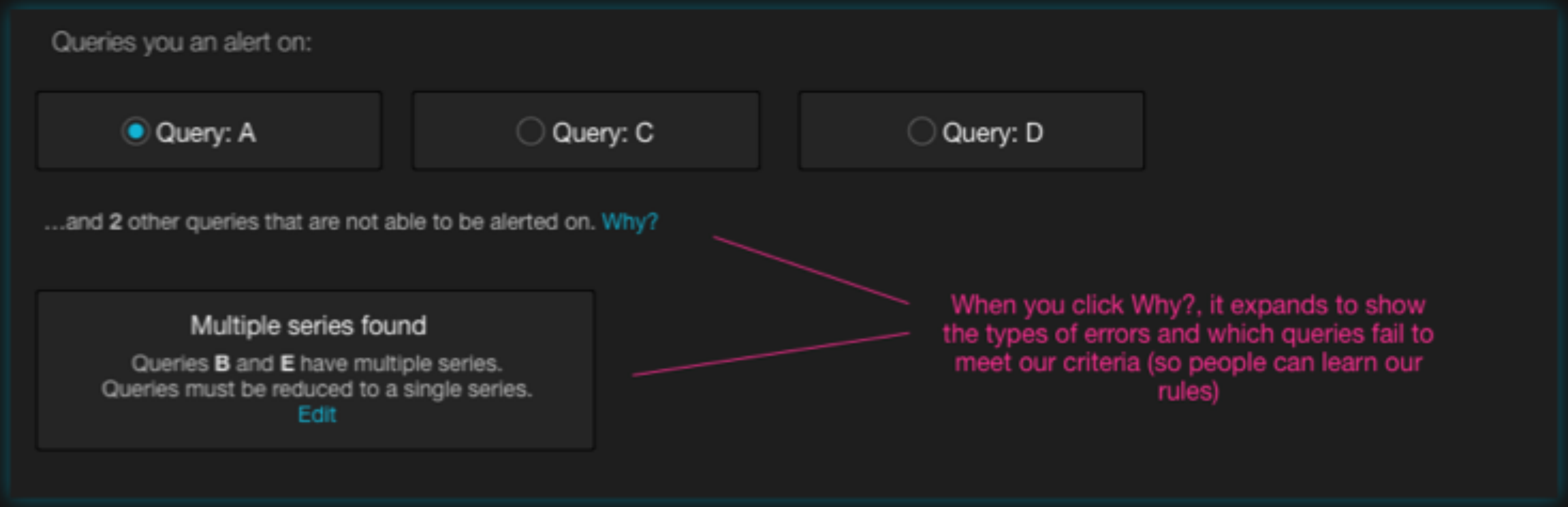


Alerting

for query

A: statsd.fakesite.counters.session_start.desktop.count

B: select mean(value) from /apps.backend.*.counters.requests.count/ where $timeFilter group by time($interval) fill(0) order asc



Queries you an alert on:

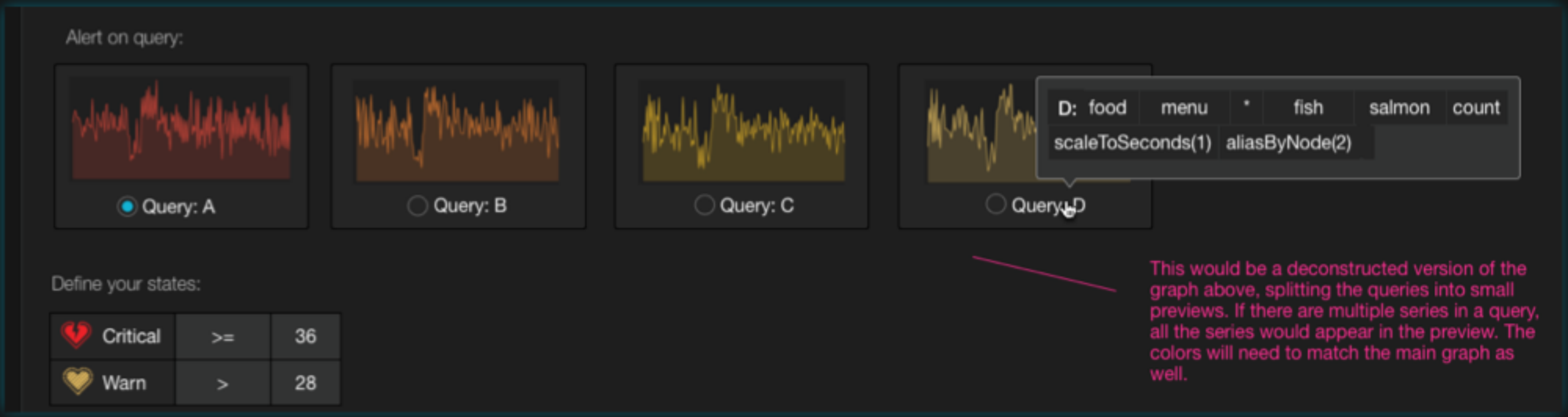
● Query: A ○ Query: C ○ Query: D

...and **2** other queries that are not able to be alerted on. Why?

Multiple series found

Queries **B** and **E** have multiple series.
Queries must be reduced to a single series.
Edit

When you click Why?, it expands to show the types of errors and which queries fail to meet our criteria (so people can learn our rules)



Alert on query:

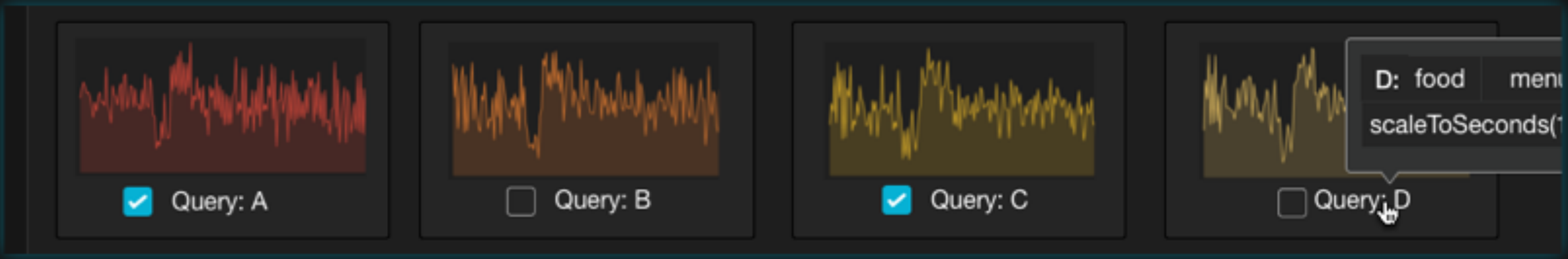
● Query: A ○ Query: B ○ Query: C ○ Query: D

D: food menu * fish salmon count
scaleToSeconds(1) aliasByNode(2)

Define your states:

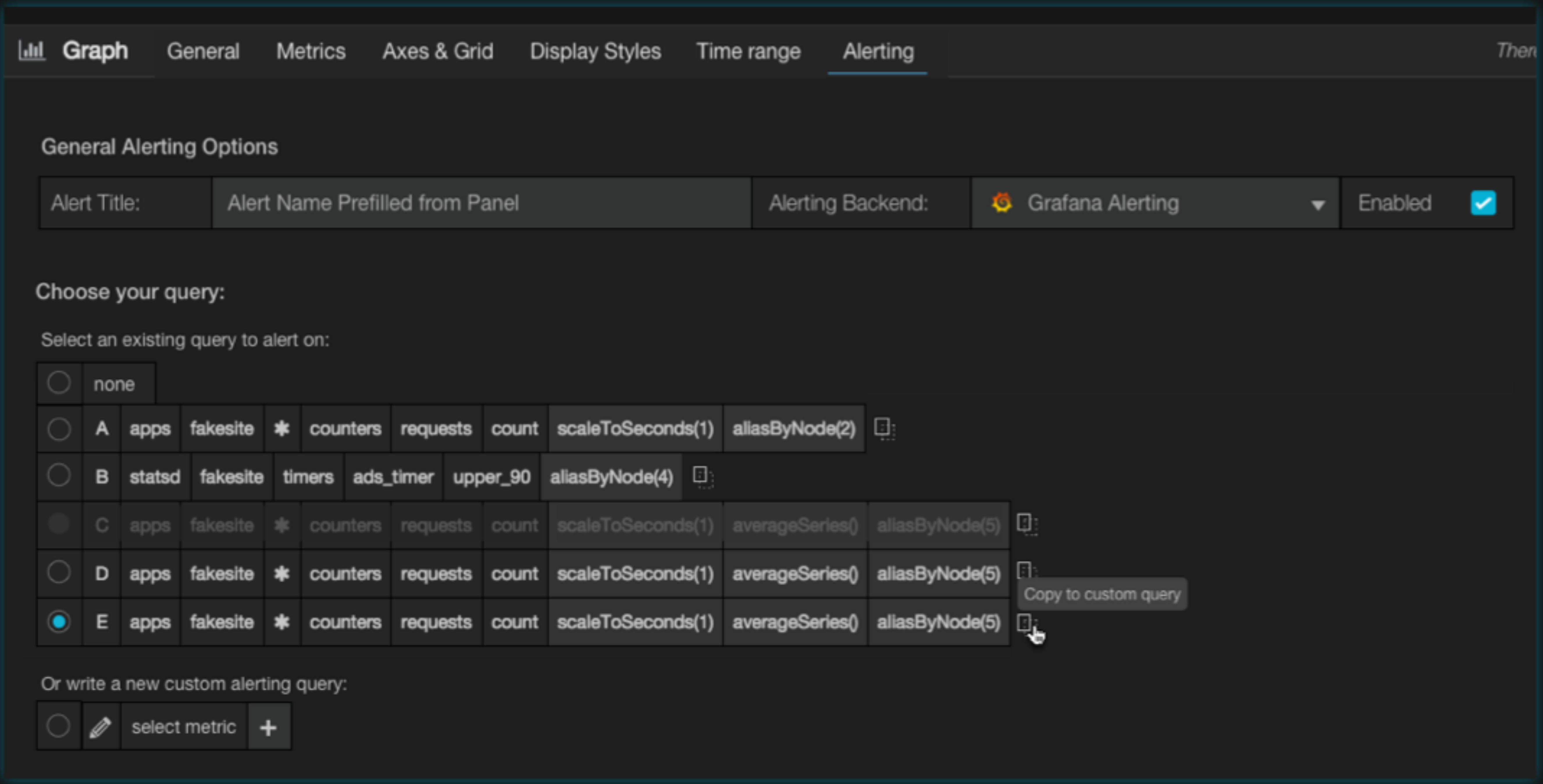
Critical	>=	36
Warn	>	28

This would be a deconstructed version of the graph above, splitting the queries into small previews. If there are multiple series in a query, all the series would appear in the preview. The colors will need to match the main graph as well.



☑ Query: A □ Query: B ☑ Query: C □ Query: D

D: food men
scaleToSeconds(



General Alerting Options

Alert Title: Alert Name Prefilled from Panel

Alerting Backend: Grafana Alerting

Enabled ☑

Choose your query:

Select an existing query to alert on:

○ none

○ A apps fakesite ✱ counters requests count scaleToSeconds(1) aliasByNode(2)

○ B statsd fakesite timers ads_timer upper_90 aliasByNode(4)

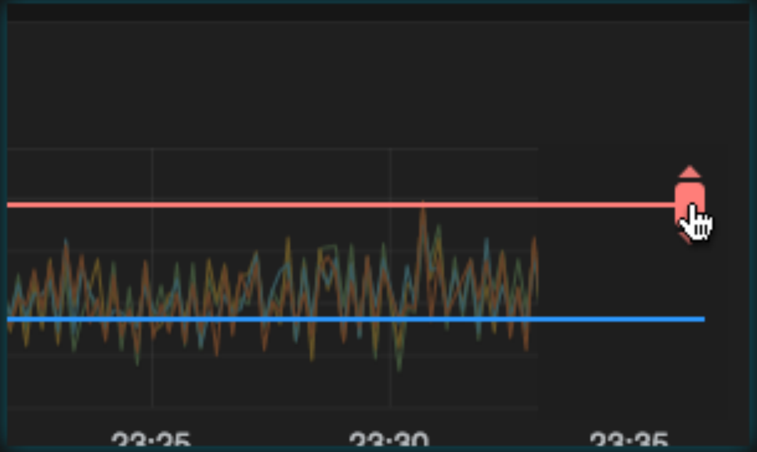
● C apps fakesite ✱ counters requests count scaleToSeconds(1) averageSeries() aliasByNode(5)

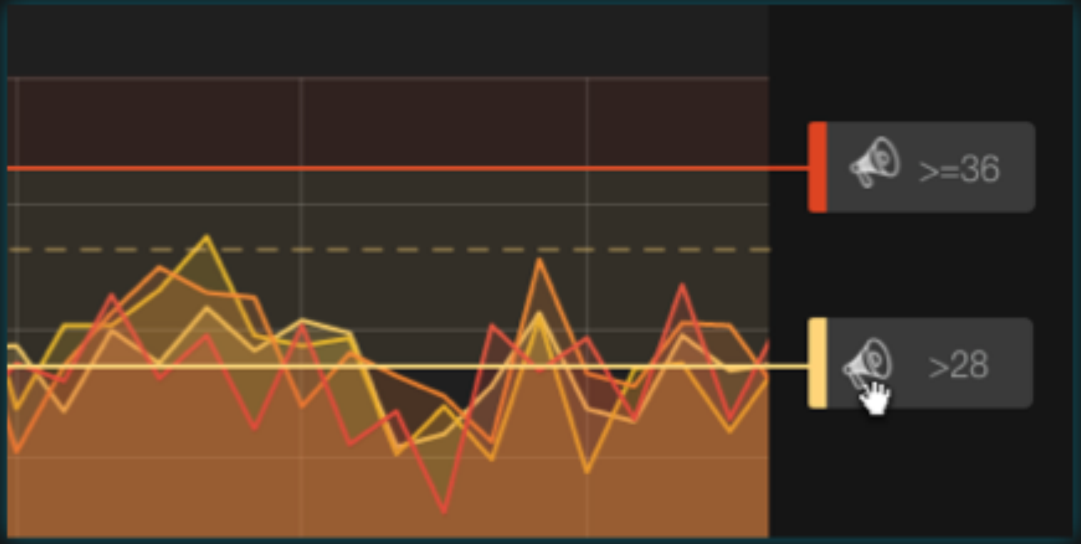
○ D apps fakesite ✱ counters requests count scaleToSeconds(1) averageSeries() aliasByNode(5)

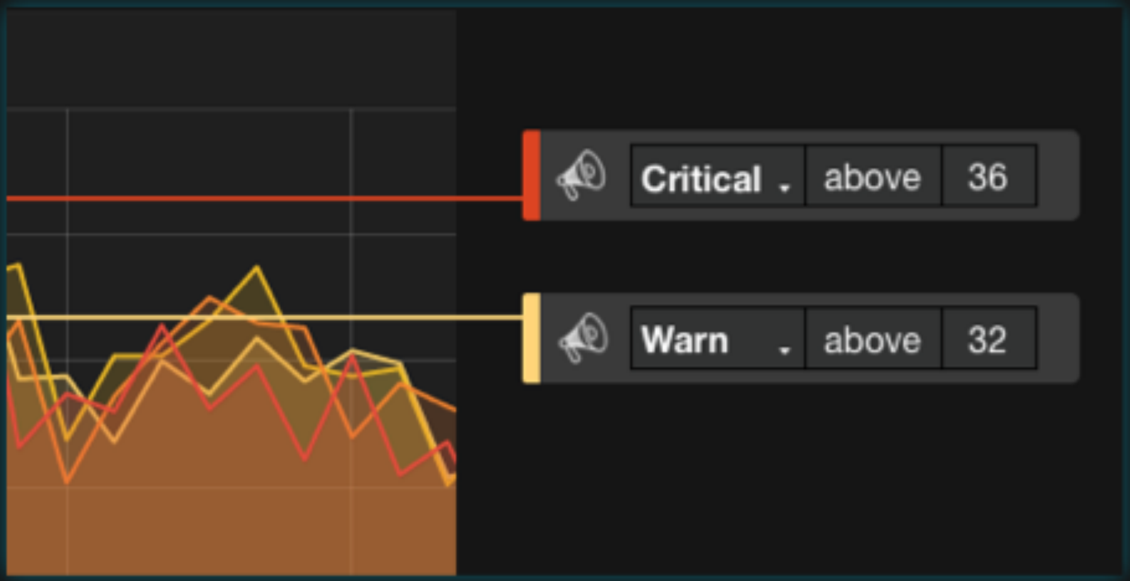
● E apps fakesite ✱ counters requests count scaleToSeconds(1) averageSeries() aliasByNode(5)

Or write a new custom alerting query:

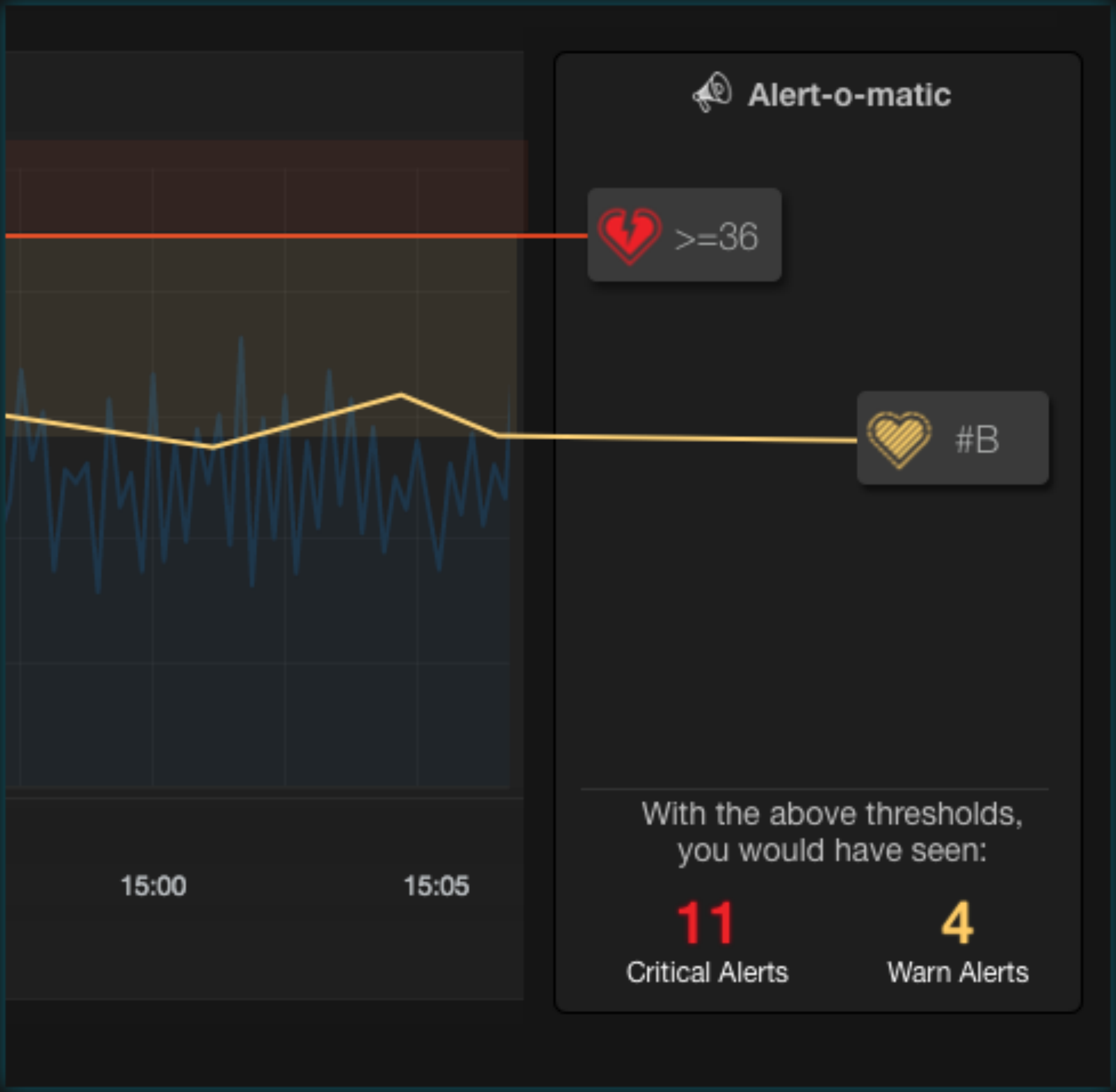
○ select metric






Critical above 36

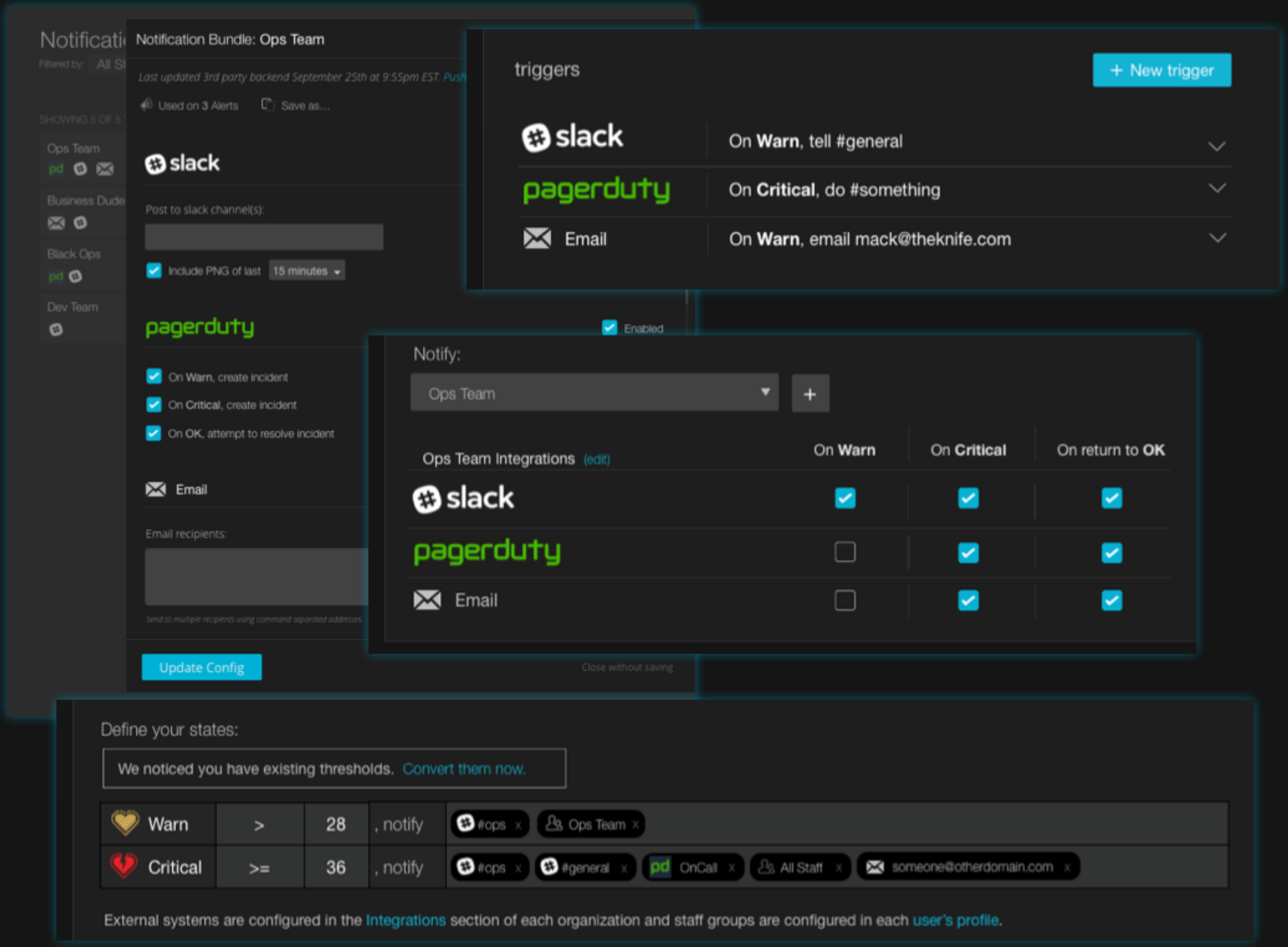
Warn above 32



With the above thresholds, you would have seen:

11 Critical Alerts

4 Warn Alerts



Notificati

Filtered by: All St

SHOWING 5 OF 5

Ops Team
pd

Business Dude

Black Ops
pd

Dev Team

Notification Bundle: Ops Team

Last updated 3rd party backend September 25th at 9:55pm EST. Push

Used on 3 Alerts   Save as...

slack

Post to slack channel(s):

☑ Include PNG of last 15 minutes

pagerduty   ☑ Enabled

☑ On **Warn**, create incident

☑ On **Critical**, create incident

☑ On **OK**, attempt to resolve incident

Email

Email recipients:

Send to multiple recipients using command separated addresses.

Update Config   Close without saving

triggers   + New trigger

slack	On **Warn**, tell #general
pagerduty	On **Critical**, do #something
Email	On **Warn**, email mack@theknife.com

Notify:

Ops Team ▾ +

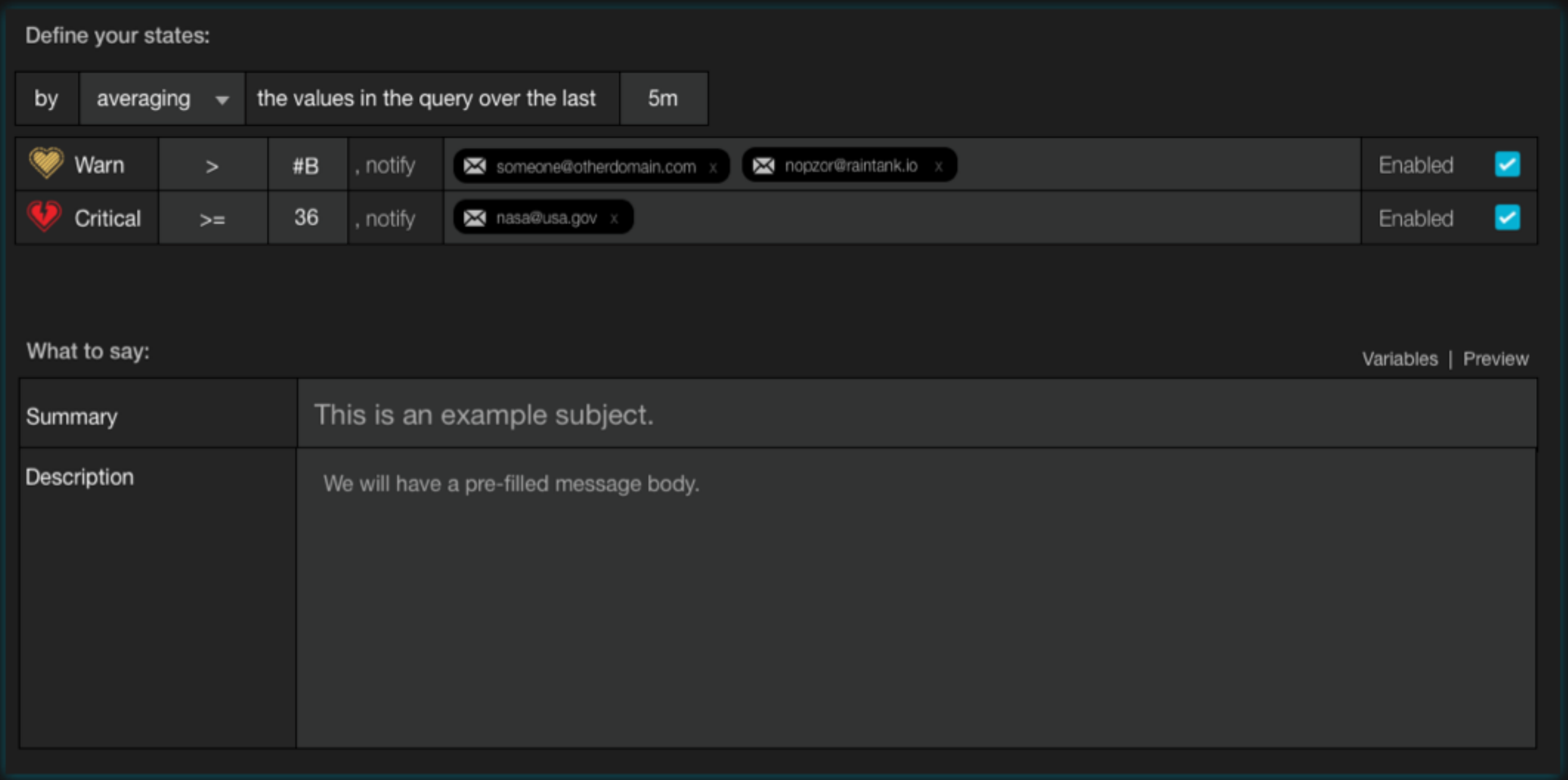
Ops Team Integrations (edit)	On **Warn**	On **Critical**	On return to **OK**
slack	☑	☑	☑
pagerduty	□	☑	☑
Email	□	☑	☑

Define your states:

We noticed you have existing thresholds. Convert them now.

Warn	>	28	, notify	#ops x Ops Team x
Critical	>=	36	, notify	#ops x #general x pd OnCall x All Staff x someone@otherdomain.com x

External systems are configured in the Integrations section of each organization and staff groups are configured in each user's profile.



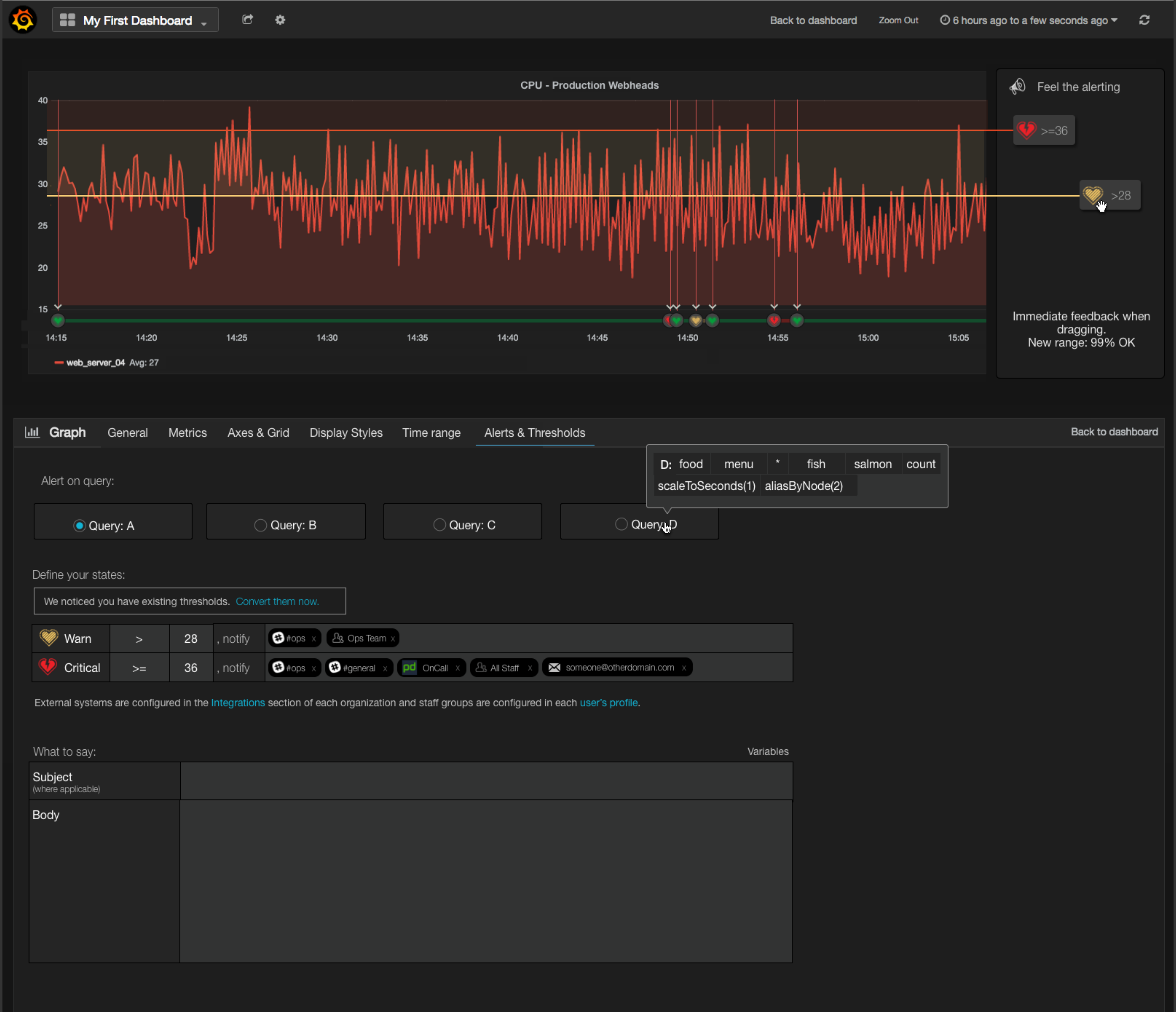
Define your states:

by	averaging ▾	the values in the query over the last	5m

♥ Warn	>	#B	, notify	✉ someone@otherdomain.com x ✉ nopzor@raintank.io x	Enabled	☑
♥ Critical	>=	36	, notify	✉ nasa@usa.gov x	Enabled	☑

What to say:

Summary	This is an example subject.
Description	We will have a pre-filled message body.



Immediate feedback when dragging.
New range: 99% OK

D: food menu * fish salmon count
scaleToSeconds(1) aliasByNode(2)

Alert on query:

● Query: A ○ Query: B ○ Query: C ○ Query: D

Define your states:

We noticed you have existing thresholds. Convert them now.

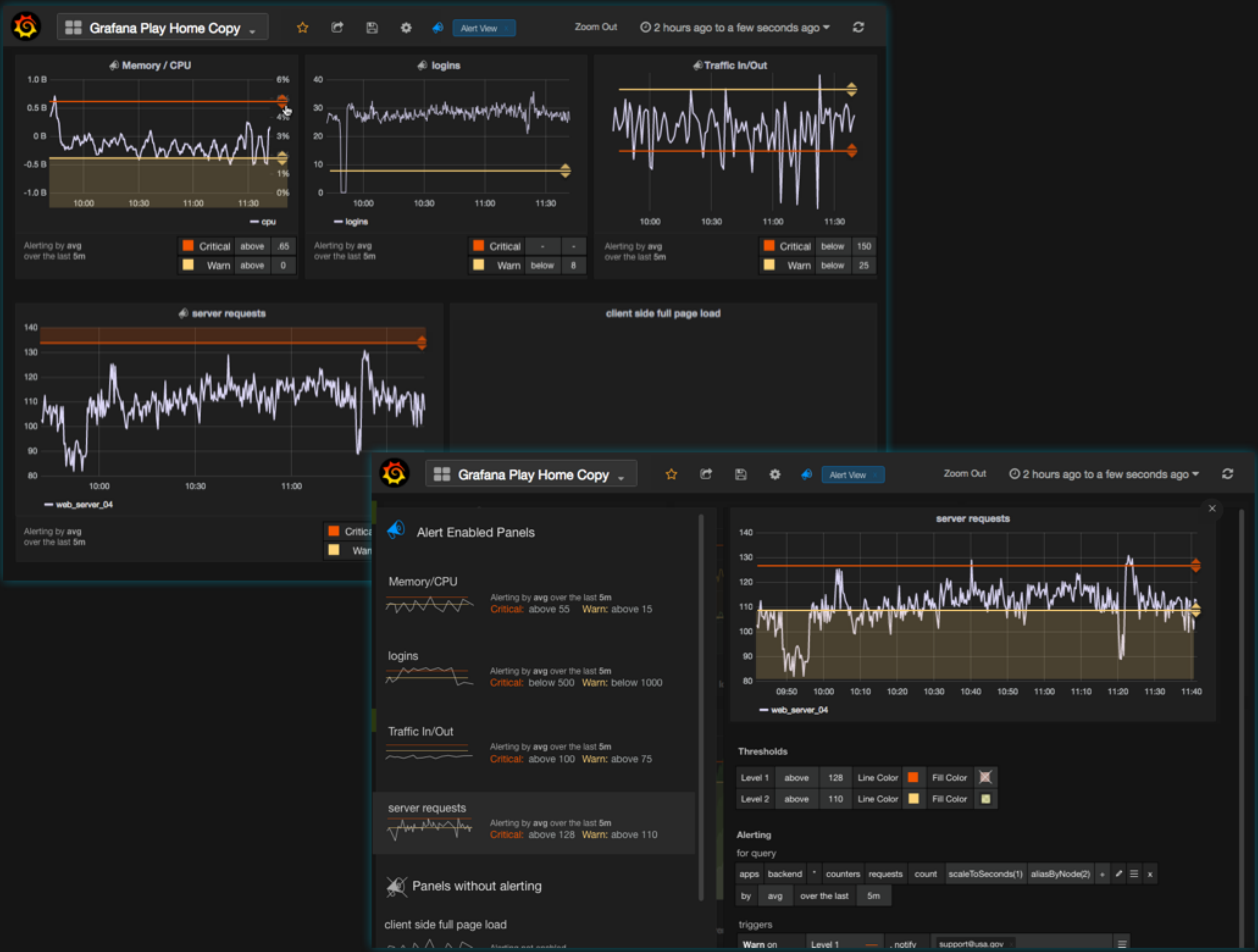
Warn	>	28	, notify	#ops x Ops Team x
Critical	>=	36	, notify	#ops x #general x pd OnCall x All Staff x someone@otherdomain.com x

External systems are configured in the Integrations section of each organization and staff groups are configured in each user's profile.

What to say: Variables

Subject (where applicable)	
Body	

Dashboard level



Memory / CPU: Alerting by avg over the last 5m

🟧	Critical	above	.65
🟨	Warn	above	0

logins: Alerting by avg over the last 5m

🟧	Critical	-	-
🟨	Warn	below	8

Traffic In/Out: Alerting by avg over the last 5m

🟧	Critical	below	150
🟨	Warn	below	25

server requests: Alerting by avg over the last 5m

🟧	Critica
🟨	Wan

Alert Enabled Panels

Memory/CPU
Alerting by **avg** over the last **5m**
Critical: above 55 Warn: above 15

logins
Alerting by **avg** over the last **5m**
Critical: below 500 Warn: below 1000

Traffic In/Out
Alerting by **avg** over the last **5m**
Critical: above 100 Warn: above 75

server requests
Alerting by **avg** over the last **5m**
Critical: above 128 Warn: above 110

Panels without alerting

client side full page load
Alerting not enabled

Thresholds

Level 1	above	128	Line Color	🟧	Fill Color	☒
Level 2	above	110	Line Color	🟨	Fill Color	🟨

Alerting

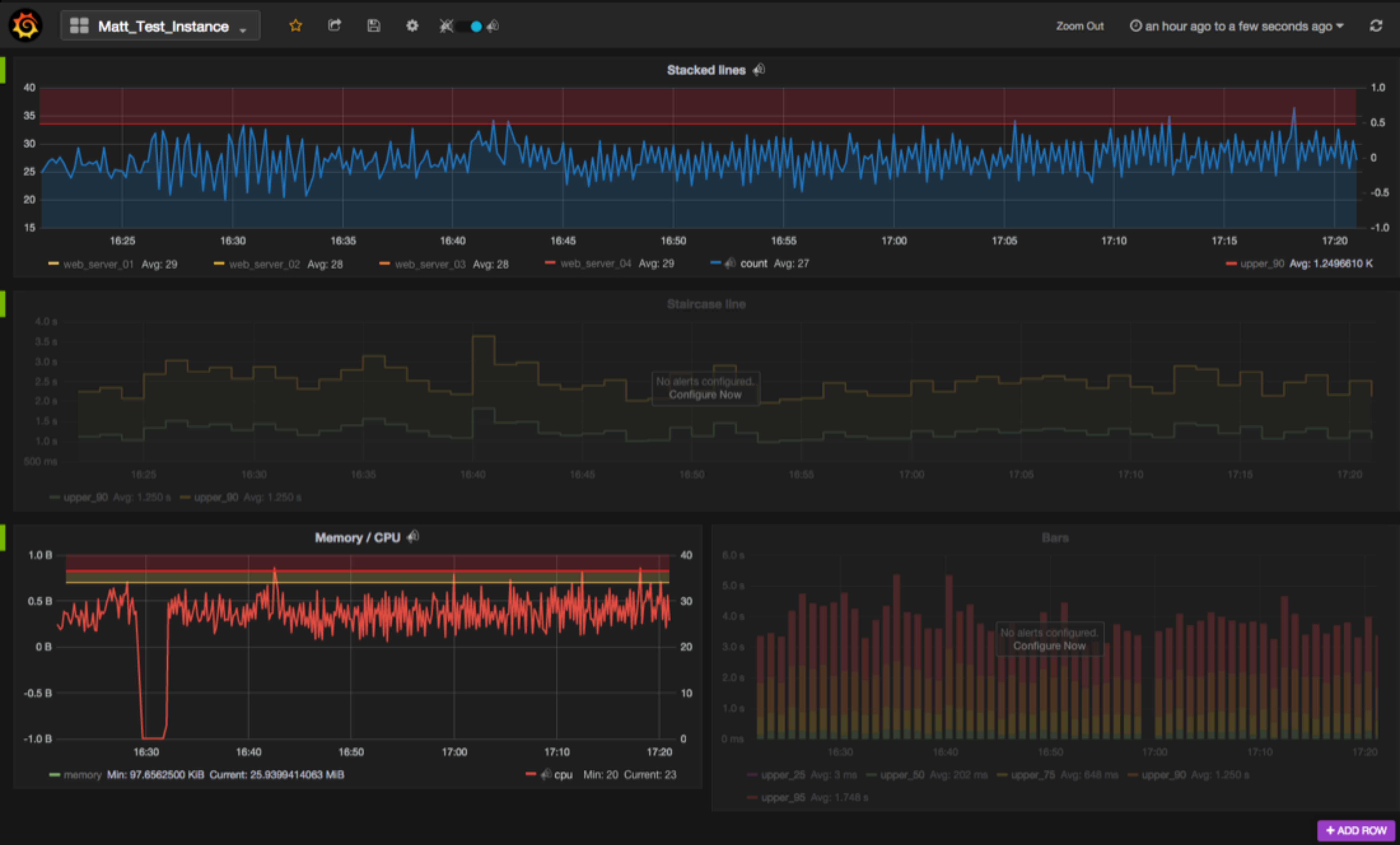
for query

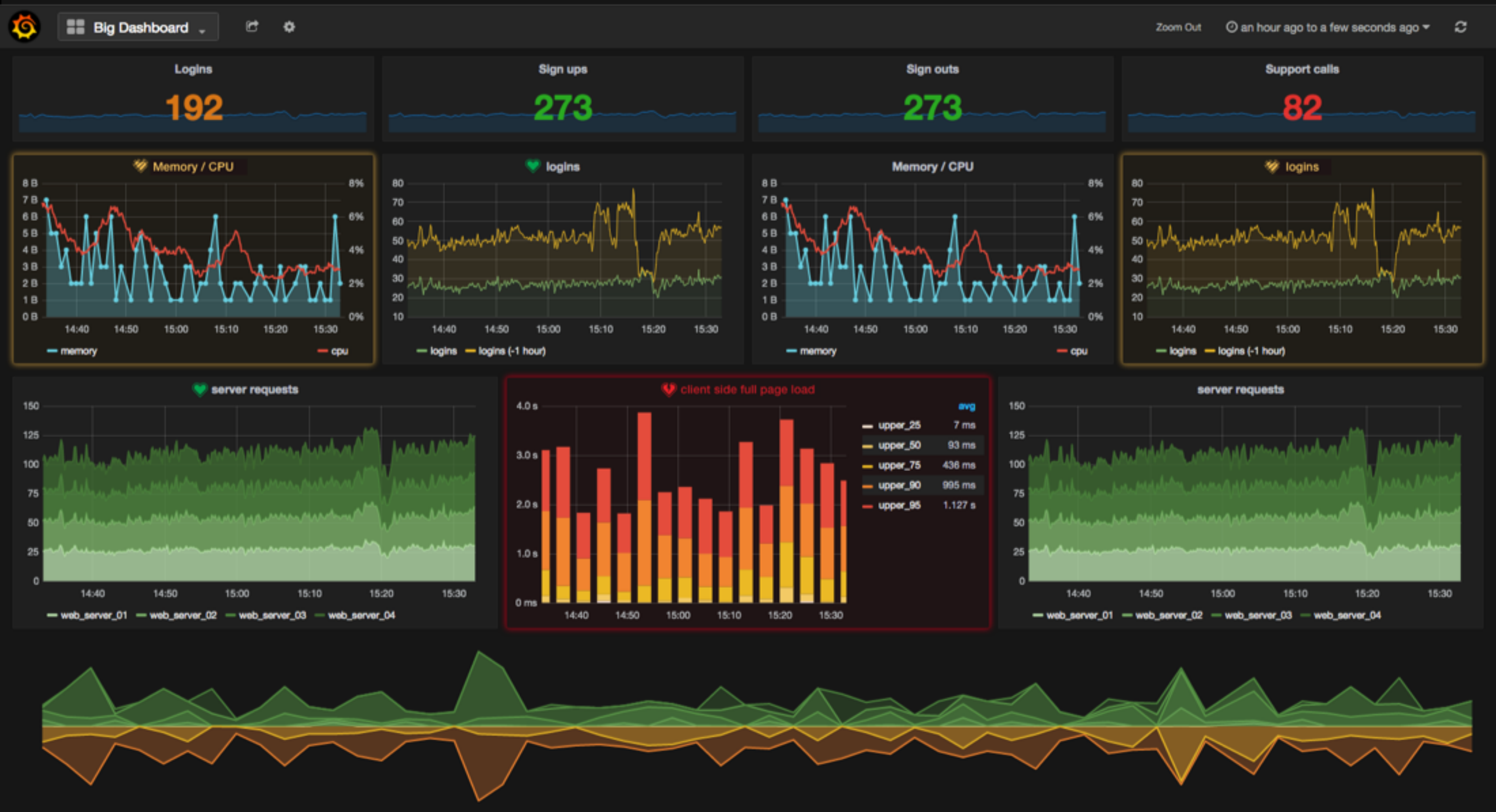
apps backend * counters requests count scaleToSeconds(1) aliasByNode(2)

by avg over the last 5m

triggers

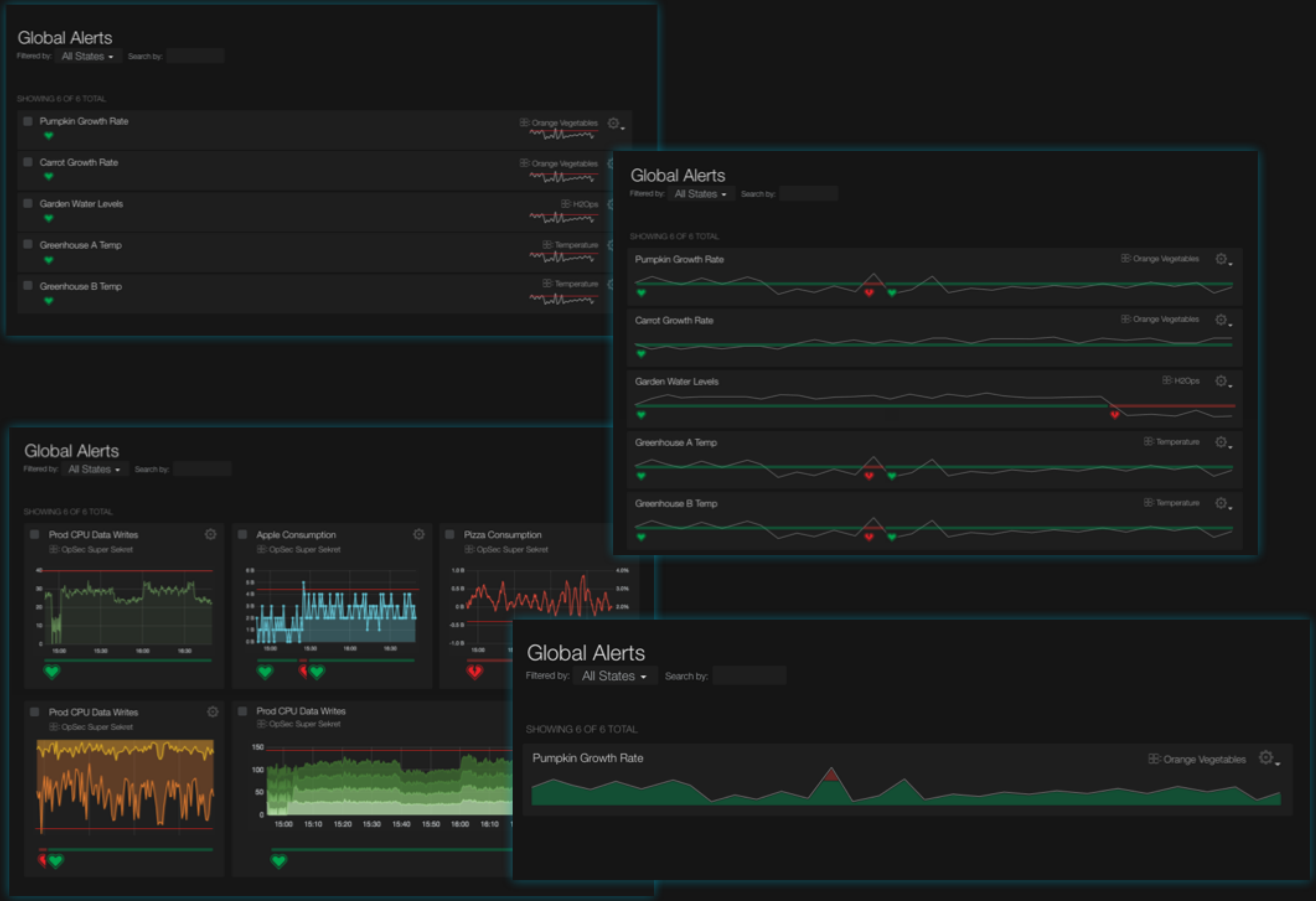
Warn on Level 1 , notify support@usa.gov


Matt_Test_Instance
Zoom Out
an hour ago to a few seconds ago
Stacked lines
40
35
30
25
20
15
1.0
0.5
0
-0.5
-1.0
16:25
16:30
16:35
16:40
16:45
16:50
16:55
17:00
17:05
17:10
17:15
17:20
web_server_01 Avg: 29
web_server_02 Avg: 28
web_server_03 Avg: 28
web_server_04 Avg: 29
count Avg: 27
upper_90 Avg: 1.2496610 K
Staircase line
4.0 s
3.5 s
3.0 s
2.5 s
2.0 s
1.5 s
1.0 s
500 ms
No alerts configured.
Configure Now
upper_90 Avg: 1.250 s
upper_90 Avg: 1.250 s
Memory / CPU
1.0 B
0.5 B
0 B
-0.5 B
-1.0 B
40
30
20
10
0
16:30
16:40
16:50
17:00
17:10
17:20
memory Min: 97.6562500 KiB Current: 25.9399414063 MiB
cpu Min: 20 Current: 23
Bars
6.0 s
5.0 s
4.0 s
3.0 s
2.0 s
1.0 s
0 ms
No alerts configured.
Configure Now
upper_25 Avg: 3 ms
upper_50 Avg: 202 ms
upper_75 Avg: 648 ms
upper_90 Avg: 1.250 s
upper_95 Avg: 1.748 s
+ ADD ROW



	avg
upper_25	7 ms
upper_50	93 ms
upper_75	436 ms
upper_90	995 ms
upper_95	1.127 s

Global level



Global Alerts

Filtered by: All States ▾ Search by:

SHOWING 6 OF 6 TOTAL

□ Pumpkin Growth Rate	Orange Vegetables
□ Carrot Growth Rate	Orange Vegetables
□ Garden Water Levels	H2Ops
□ Greenhouse A Temp	Temperature
□ Greenhouse B Temp	Temperature

Global Alerts

Filtered by: All States ▾ Search by:

SHOWING 6 OF 6 TOTAL

Pumpkin Growth Rate	Orange Vegetables
Carrot Growth Rate	Orange Vegetables
Garden Water Levels	H2Ops
Greenhouse A Temp	Temperature
Greenhouse B Temp	Temperature

Global Alerts

Filtered by: All States ▾ Search by:

SHOWING 6 OF 6 TOTAL

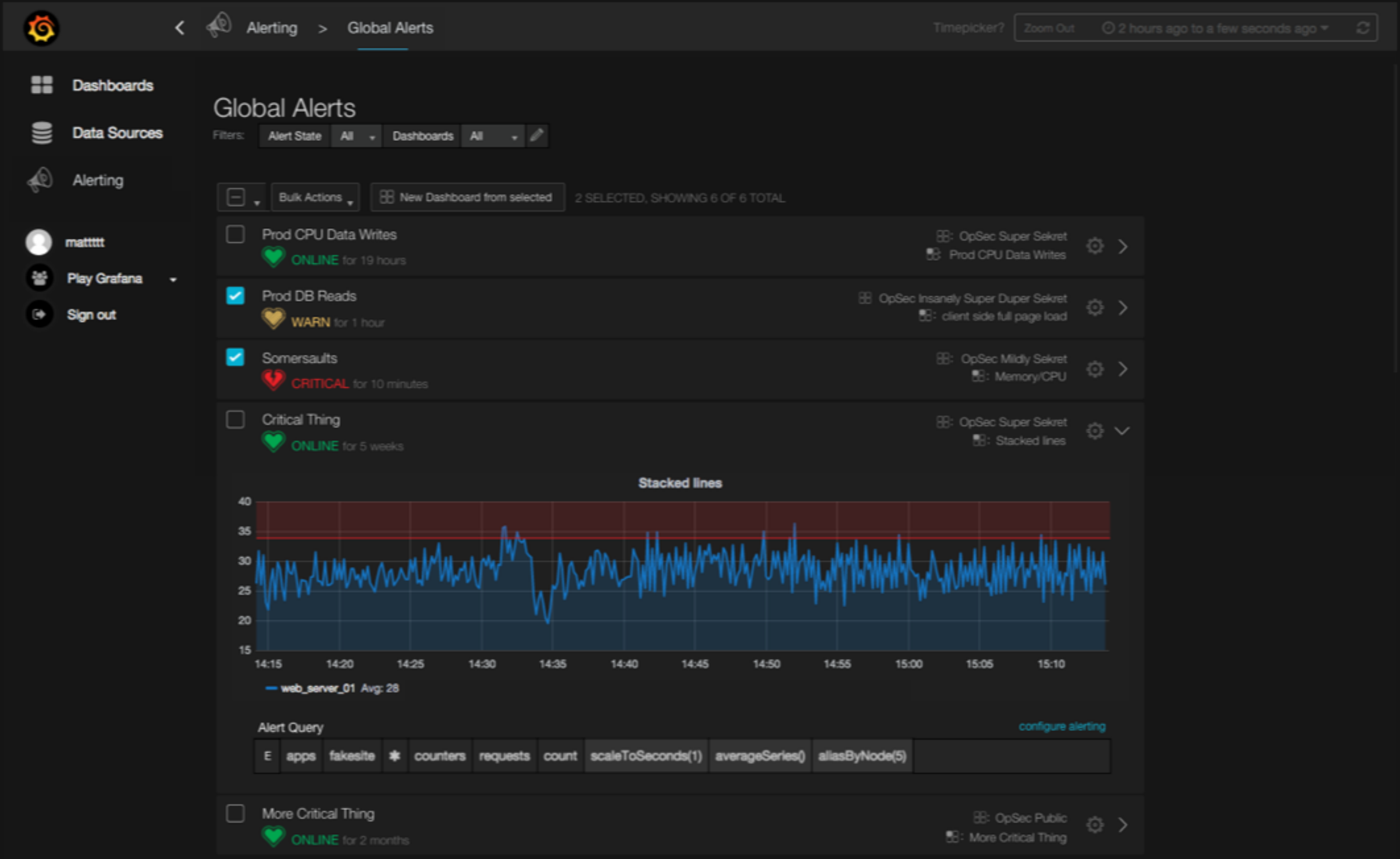
□ Prod CPU Data Writes	OpSec Super Sekret
□ Apple Consumption	OpSec Super Sekret
□ Pizza Consumption	OpSec Super Sekret
□ Prod CPU Data Writes	OpSec Super Sekret
□ Prod CPU Data Writes	OpSec Super Sekret

Global Alerts

Filtered by: All States ▾ Search by:

SHOWING 6 OF 6 TOTAL

Pumpkin Growth Rate	Orange Vegetables



Global Alerts

Filters: Alert State All Dashboards All

2 SELECTED, SHOWING 6 OF 6 TOTAL

□ Prod CPU Data Writes
ONLINE for 19 hours
OpSec Super Sekret
Prod CPU Data Writes

☑ Prod DB Reads
WARN for 1 hour
OpSec Insanely Super Duper Sekret
client side full page load

☑ Somersaults
CRITICAL for 10 minutes
OpSec Mildy Sekret
Memory/CPU

□ Critical Thing
ONLINE for 5 weeks
OpSec Super Sekret
Stacked lines

Alert Query

configure alerting

E apps fakesite * counters requests count scaleToSeconds(1) averageSeries() aliasByNode(5)

□ More Critical Thing
ONLINE for 2 months
OpSec Public
More Critical Thing

Grafana:

data viz

alert config

alert state viz

Grafana:

data viz

alert config

alert state viz

Handler:

alert scheduling

alert execution

notifications

grafana api → handler

bosun.org
nagios.org
sensuapp.org
github.com/arachnys/cabot
github.com/scobal/seyren
...

“batteries included, but removeable”

Time to vote

Why alerting IN Grafana

why:

unified workflow

why:

integration

why:

power through UX

Conclusion

- Workflow is key
- Composability & compatibility
- Handler integrations. <3 community.
- Prototype coming in Grafana 2.x

Q&A

https://github.com/grafana/grafana/issues/2209