

Once Upon a Time...



**Alerts don't suck.
YOUR alerts suck!**

@LeonAdato
Principal Technical Evangelist





Leon Adato

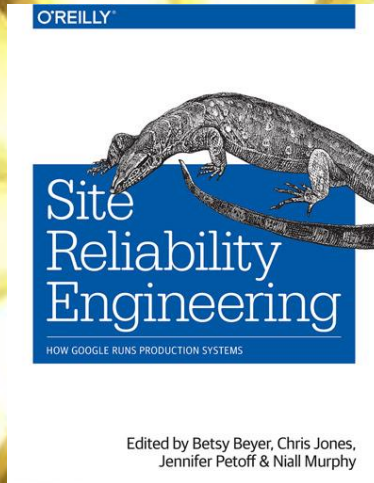
- Principal Technical Evangelist
 - **at Kentik**
- ~35 yrs in tech.
- ~25 yrs monitoring & observability.
- ~10 yrs as a Tech Evangelist, DevRel Advocate, and (ugh) “Head Geek”.
- Tivoli, BMC, OpenView, janky perl scripts, Nagios, SolarWinds, DOS batch files, Zabbix, Grafana, New Relic, and other assorted nightmare fuel.

@LeonAdato on almost all social media.

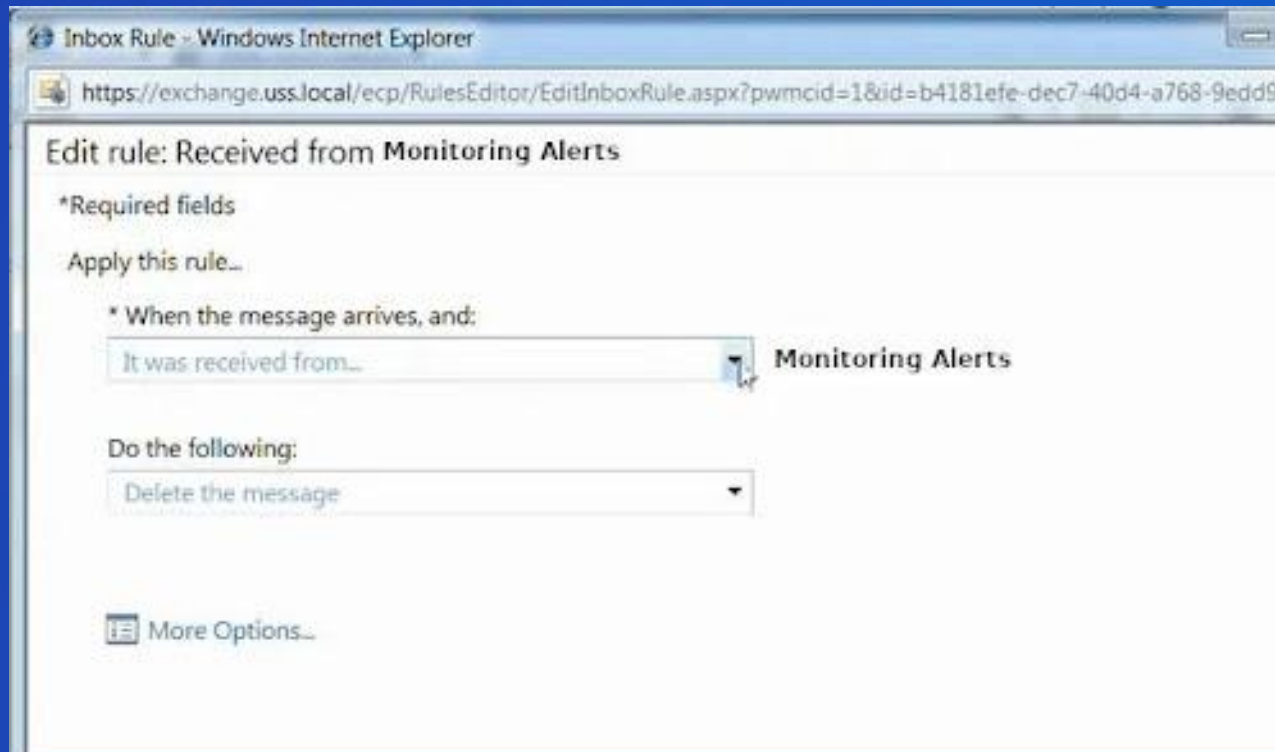
This is an Oyster Talk™



The Good Book Says....



Inbox rules are like a\$\$holes...*



** Everyone has one, and they all stink*

A hill I will die on



"¿Ke es esta medra?" - Leon's Abuela



**Bring family together
with Lipton® Soup!**

Warm, soothing and satisfying since 1940

Stovetop Directions:
Makes 4 Cups

- 1 In medium saucepan, bring 4 cups (32 oz) water to boil; stir in contents of one pouch soup mix.
- 2 Reduce heat and simmer uncovered, stirring occasionally, 5 minutes or until noodles are tender.

Caution: Soup May Be Hot.
Refrigerate Any Unused Cooked Portion.

Microwave Directions:
Makes 4 Cups

- 1 In 2-quart microwave-safe casserole, combine 4 cups (32 oz) water and contents of one pouch soup mix.
- 2 Microwave uncovered at HIGH 10 to 12 minutes* or until noodles are tender, stirring once halfway through cooking.

* Microwave ovens vary; adjust times as needed.

For more recipes go to:
[Yummly.com/liptonsoup](https://www.Yummly.com/liptonsoup)

Easy Homemade Soup
Minestrone

Ingredients:

- 1 carrot, thinly sliced
- 2 celery stalks, thinly sliced
- 1 small onion, chopped
- 1 clove garlic, finely chopped
- 1 tsp. dried oregano
- 1 can (15-1/2 oz) diced tomatoes
- 1 can (15-1/2 oz) cannellini or white kidney beans, drained
- 1 envelope Lipton® Soup Secrets® Ring-O-Noodle Soup Mix

1. Cook carrot, celery, and onion in a small amount of olive oil in a large saucepot until softened.
2. Stir in remaining ingredients and 3 cups water; bring to a boil. Reduce heat and simmer until noodles are tender, about 5 minutes.
3. Garnish with chopped fresh basil and Parmesan cheese.



(courtesy of Honeycomb.io)

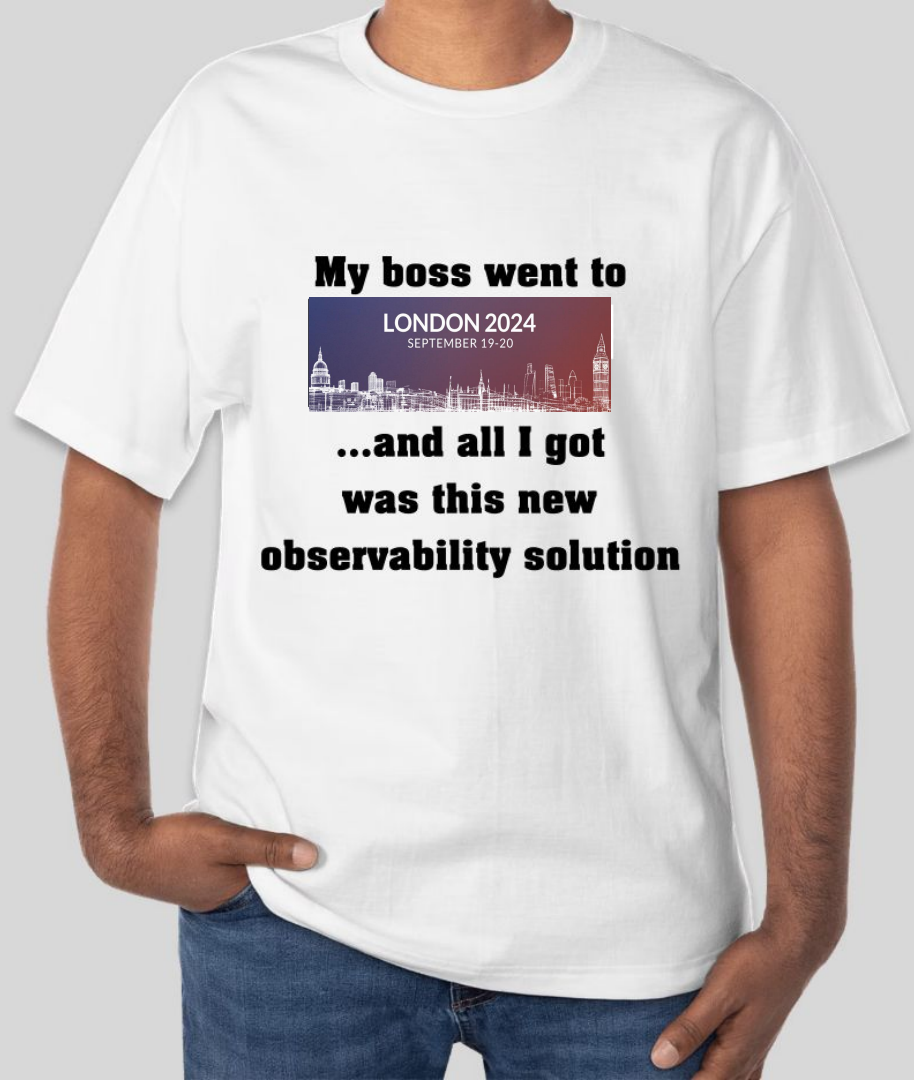
Lesson One: Alerts Are... what?!?



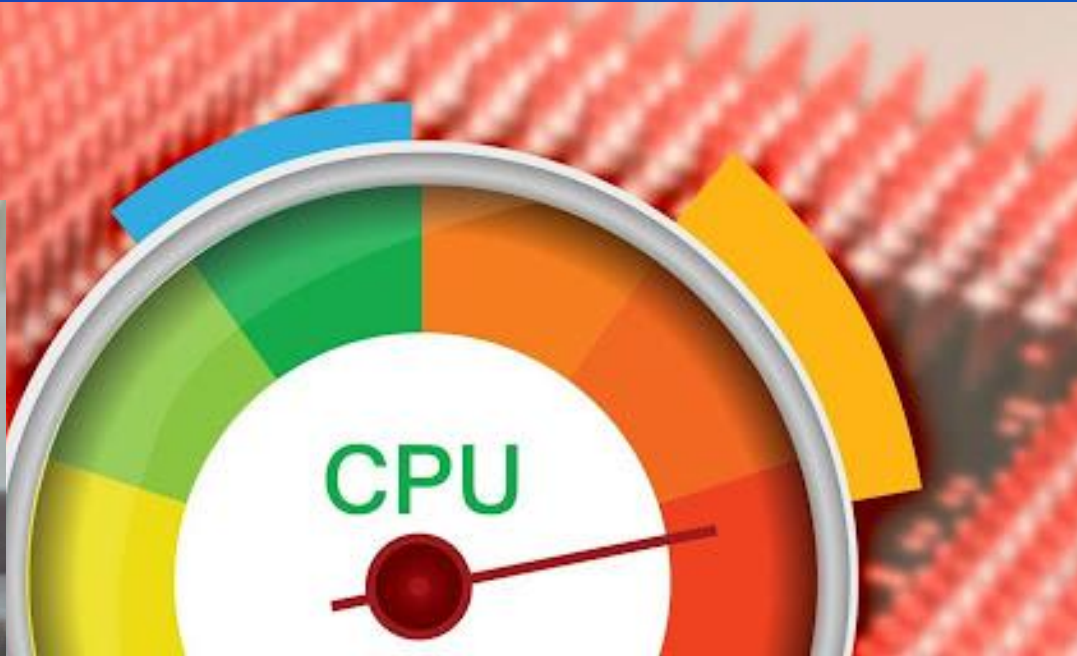
Three Important Rules:

- Alerts \leftrightarrow Monitoring
- Alerts \neq Monitoring
- Alerts \neq Monitoring

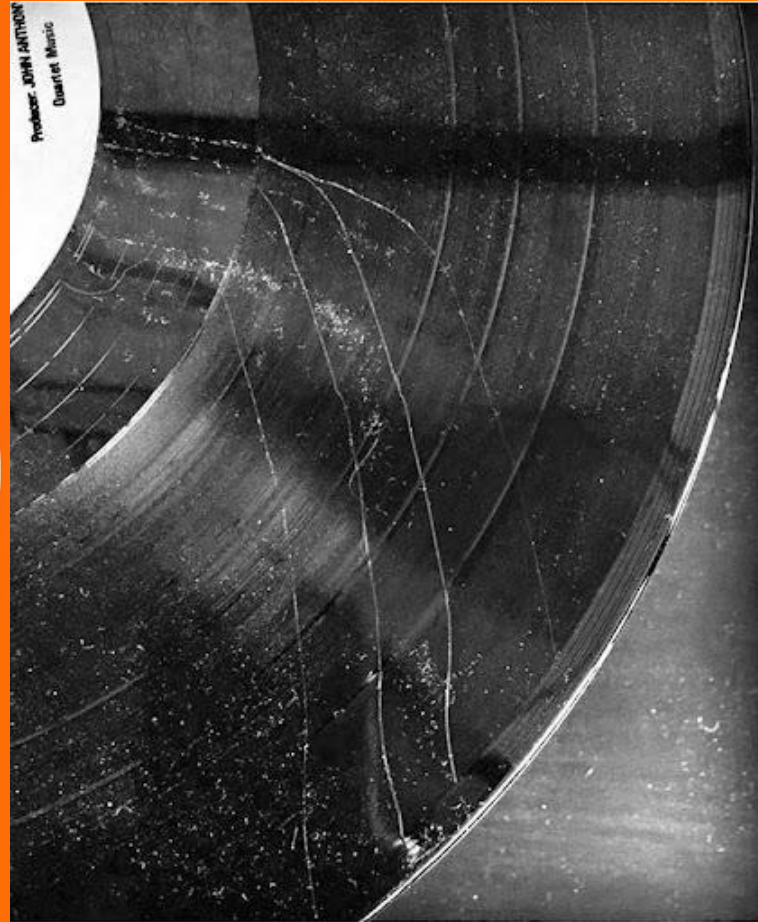
About once a year...



The problem with high CPU alerts isn't the CPU



Hold up...



Lesson Two: Monitoring vs Observability



Lesson Two:

~~Monitoring vs Observability~~

Monitoring AND Observability



Let's add a little nuance

Observability

- Un-Known Unknowns
- High cardinality
- Correlation baked-in
- Golden signals
(latency, traffic, errors, saturation)

Monitoring

- Known Unknowns
- All cardinalities welcome
- (mostly) manual correlation
- Domain-specific signals

Alerts and Observability

Observability

- Un-Known Unknowns
- High cardinality
- Correlation baked-in
- Golden signals
(latency, traffic, errors, saturation)

Alerts and Observability

Observability

- Un-Known Unknowns
- High cardinality
- Correlation baked-in
- Golden signals



Alerts and Observability

Observability

- Un-Known Unknowns
- High cardinality
- Correlation baked-in
- Golden signals



Designed by M. Scharlock

Lesson Three: Alerts Must Matter



A simple algorithm:

IFF(Human && do something && now && about \$problem) == true



IFF(Human && do something && now && about \$problem) == true

If it's not an alert,

- **(!= human)**
- **(!= now)**
- **(!= problem)**
- **(!= doing something)**

What is it?

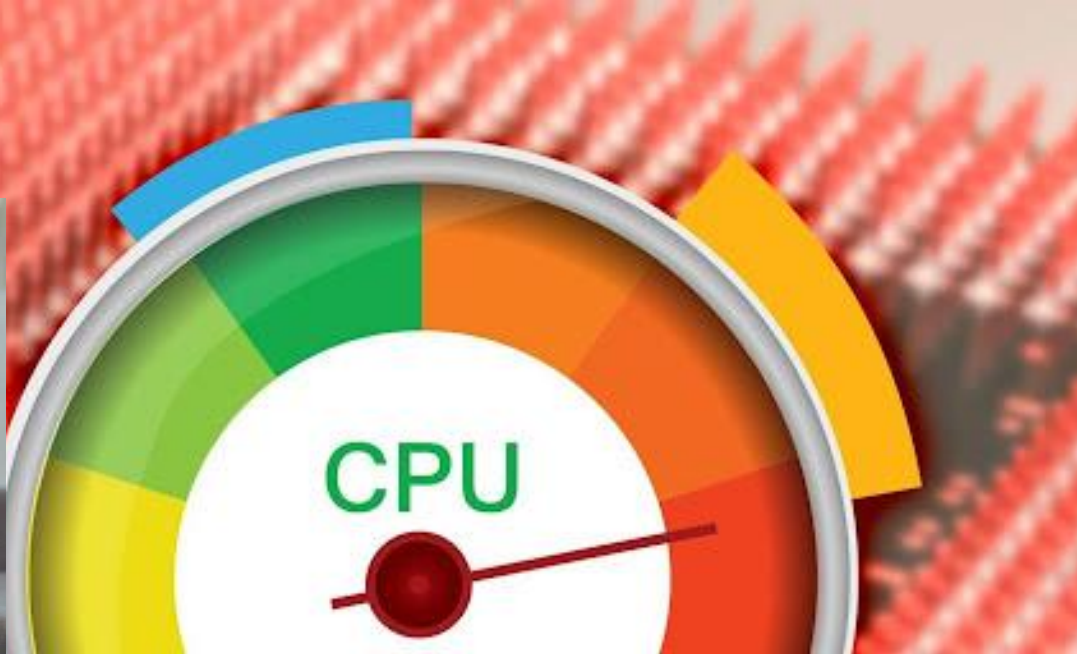
== automation

== report

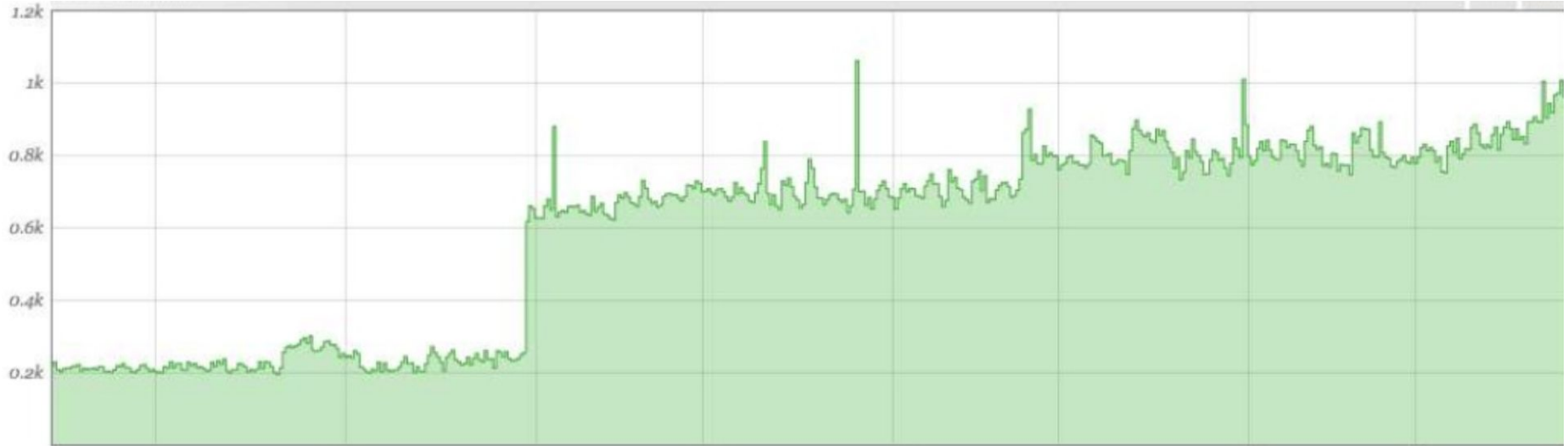
== dashboard

== delete

The problem with high CPU alerts isn't the CPU

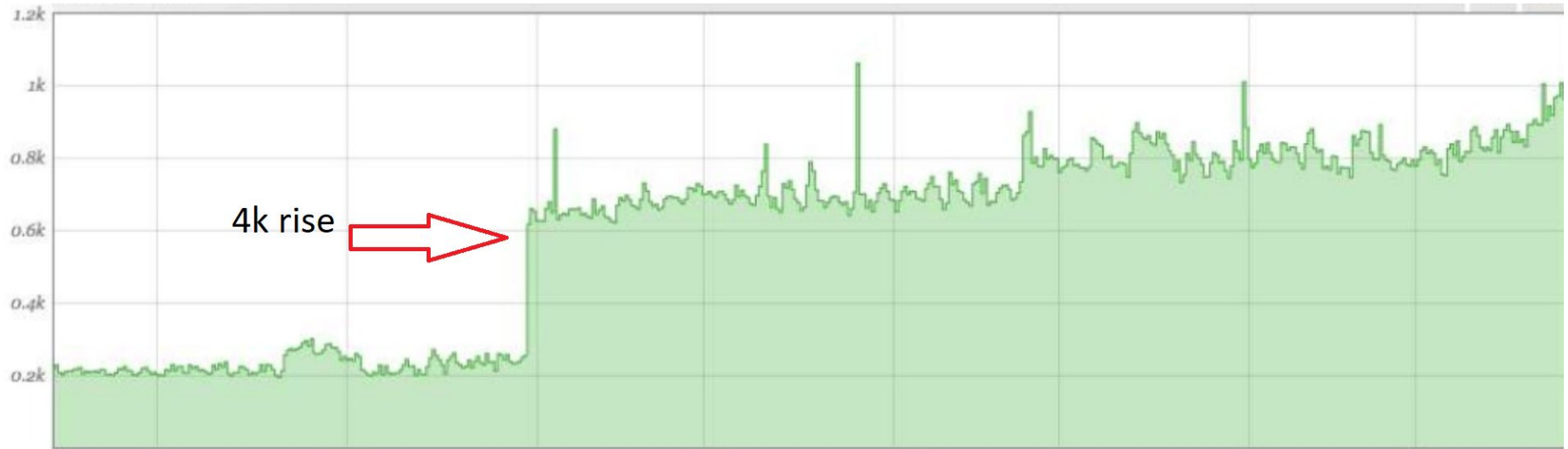


Do you see it?



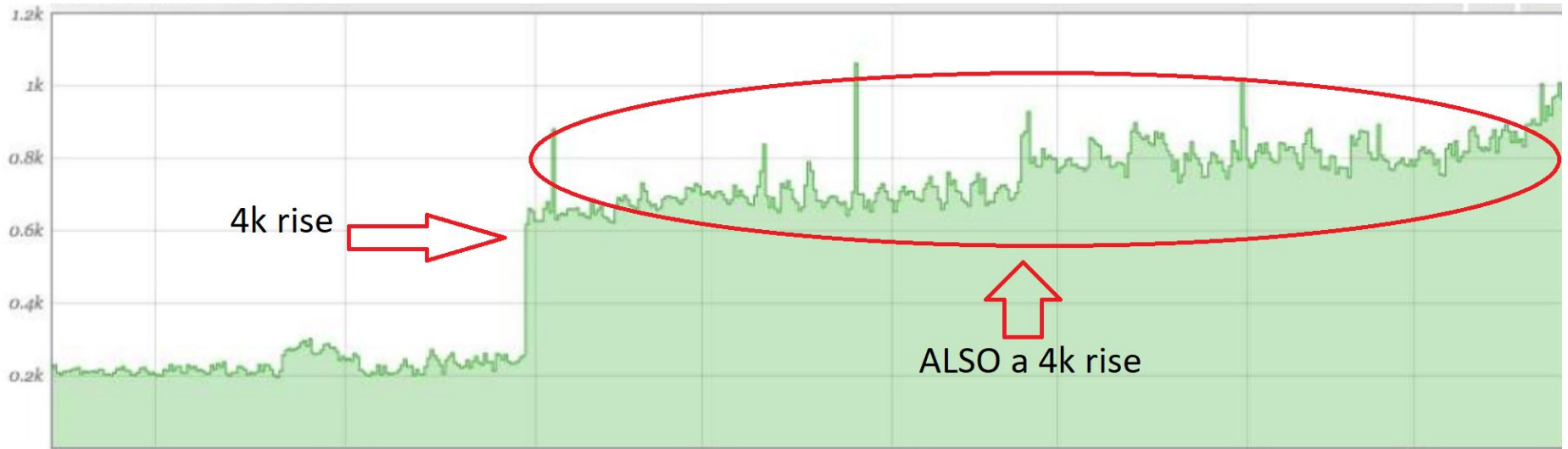
Credit: Leon Fayer

Do you see it?



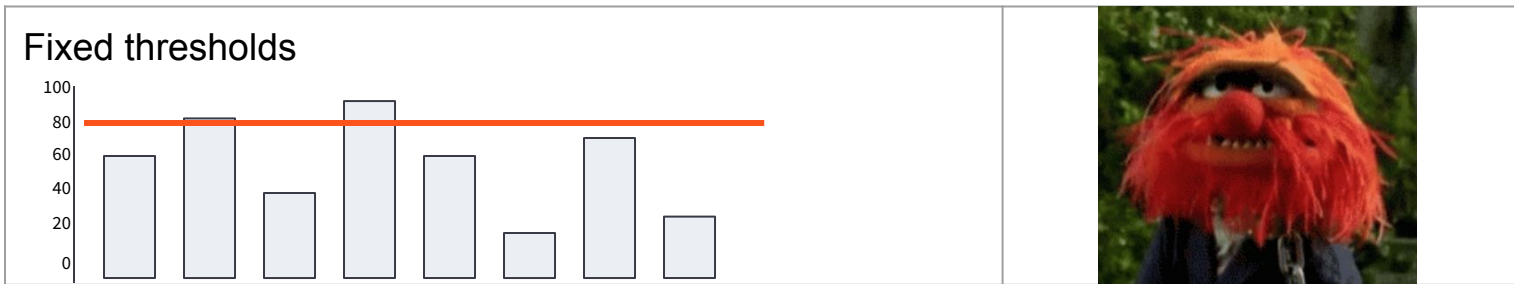
Credit: Leon Fayer

Do you see it?



Credit: Leon Fayer

Monitoring is like Music: Both need a solid baseline!



Threshold + Baseline Example

Edit Major Threshold Conditions

×

An alert will be triggered when **all** of the below conditions are met for a given key:

☒ Static Condition

Bits/s

Show Chart

If traffic is at least

☒ Baseline Condition

Bits/s

If traffic is at least the baseline.

☐ Top Keys Condition

ⓘ

 Cannot combine with a Baseline condition.

☐ Interface Capacity Condition

ⓘ

 Cannot combine with Baseline condition. Requires Interface dimension.

☐ Ratio-Based Condition

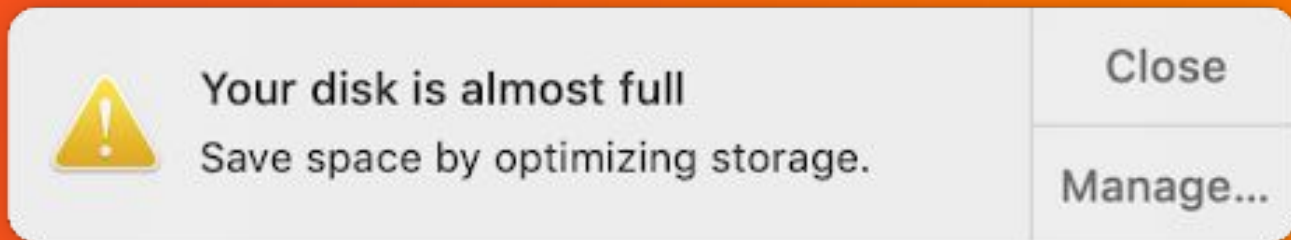
ⓘ

 Requires at least 2 metrics to be selected.

Cancel

Apply

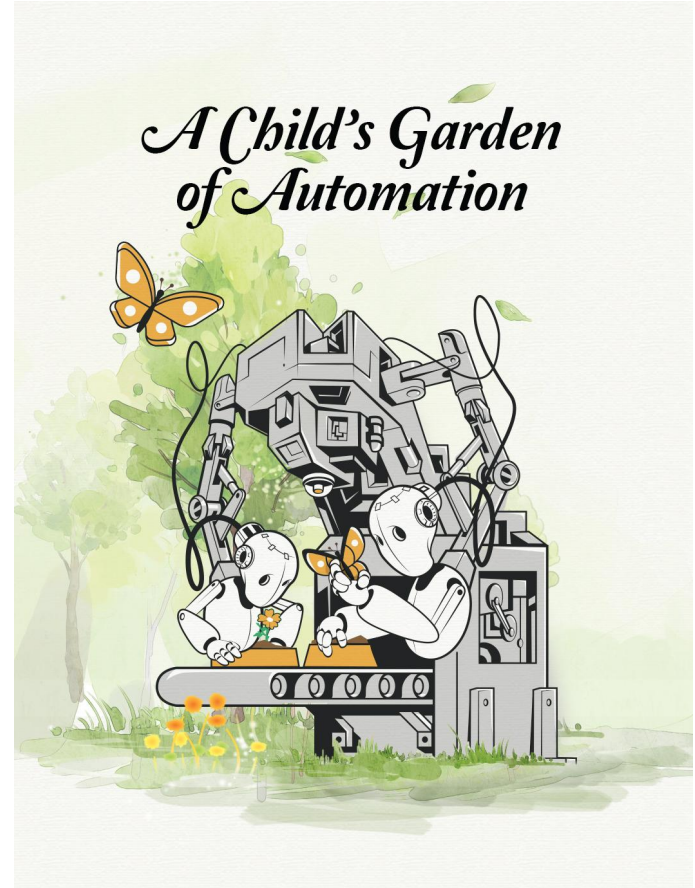
Yes, it's a problem



But what do you DO about it?

What we have here is...
...a failure to AUTOMATE

When (this thing) goes wrong,
What do YOU do about it?



A cascade of (automated) joy

IIS App is slow

**Clear the Application Pool
(wait)**

**Reset the IIS service
(wait)**

**Rebuild from image
(wait)**

**Move to new region/site/whatever
(wait)... then send ticket**

Lesson Four: Skilled Interrogati... Interviewing



Hunting the great "useful alert"

- How do YOU know when something went wrong?
- How do you know it's "all better"?
- Is there a knowledge article for it (yet)?
- Can you make it happen on purpose?

Prove value with this one weird trick!

<u>Name</u>	<u>Cost w/out</u>	<u>Cost with</u>	<u>Alert qty</u>	<u>Total Saved</u>
Order Entry Slow	\$150	\$25	23	\$2,875
Order entry down	\$500	\$125	2	\$750
Disk Full	\$275	\$20	322	\$82,110

Let's sum up:

- Identified and interrogated the recipient
- Designed alert that matters because it
 - Has real-world trigger elements
 - Takes duration and baseline into account
 - Includes automation
- Verified the alert is built with the intent of immediate action by a human
- Communicated the value to the business

Lesson Five:

The work never ends



From the Pages of the Sages

הִפֹּךְ בָּהּ וְהִפֹּךְ בָּהּ, דְּכֻלָּא בָּהּ

“Turn it over, and [again] turn it over, for all is therein.”

- Pirkei Avot (Ethics of the Fathers) 5:22

לֹא עָלֶיךָ הַמְלָאכָה לְגַמֹּר
וְלֹא אֶתָּה בֶּן חוֹרִין לְבַטֵּל מִמֶּנָּה

*“It is not your duty to finish the work,
but neither are you at liberty to neglect it.”*

- Pirkei Avot 2:16

YOU MADE IT!!!

**Get our famous
TCP/IP cap by
scanning the
QR code below:**



Are you  **IRRITATED** ?

I'm ready for your
questions!

@LeonAdato



YOU MADE IT!!!

**Get our famous
TCP/IP cap by
scanning the
QR code below:**



How Did We Get Here?



ACTUAL USER experience?
Who the FSCK knew?!?!?

Dev thinking they have
everything under control

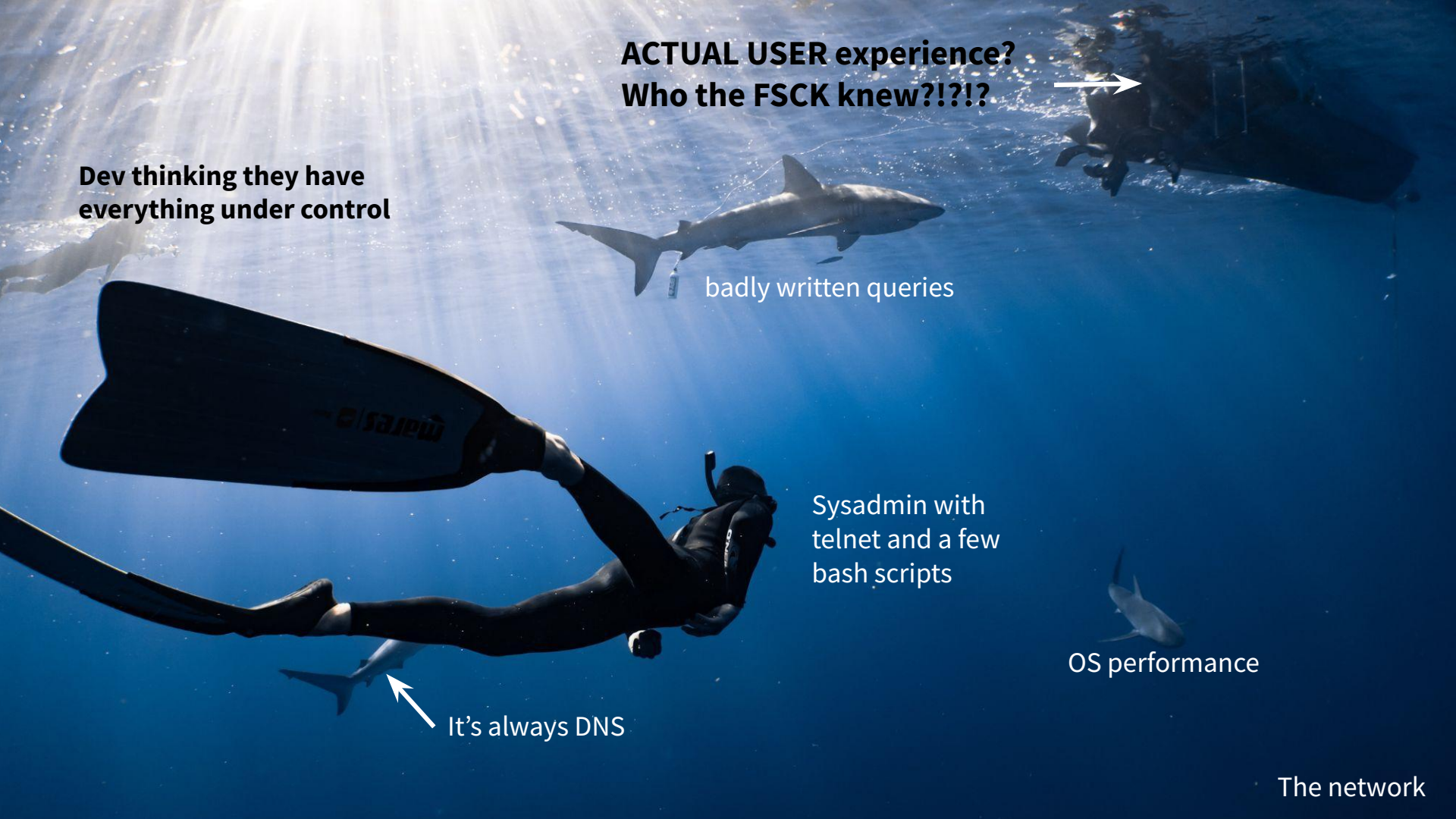
badly written queries

Sysadmin with
telnet and a few
bash scripts

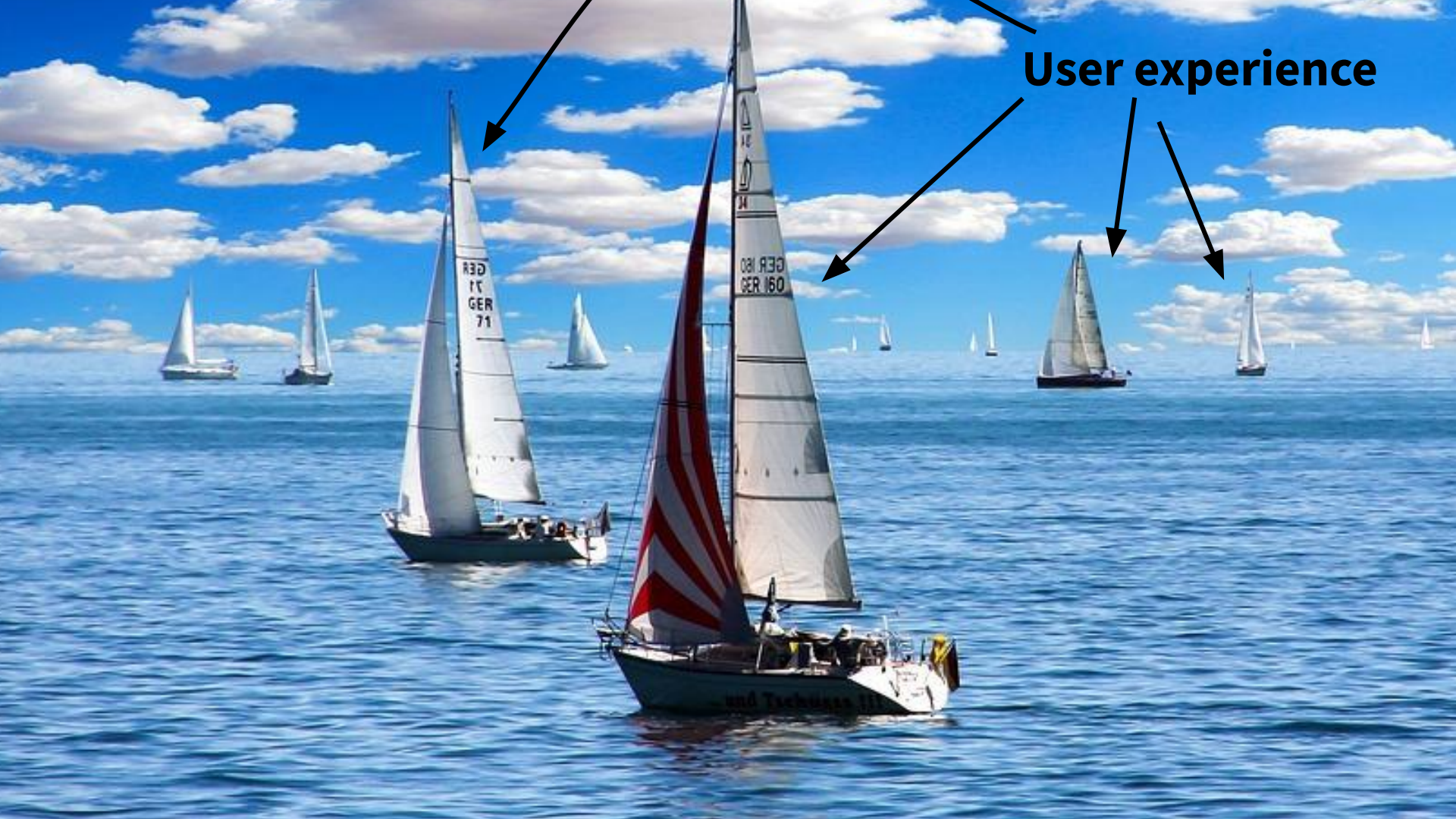
OS performance

It's always DNS

The network



User experience



Alerts represent a significant drag on the system

Query that runs every xx minutes against the ENTIRE data set

Do not overwhelm the system

"Monitoring sucks" is frequently because there are 2,000 alerts that are competing for resources.