Once Upon a Time...

Alerts don’t suck.
YOUR alerts suck!

@LeonAdato
Principal Technical Evangelist

Leon Adato

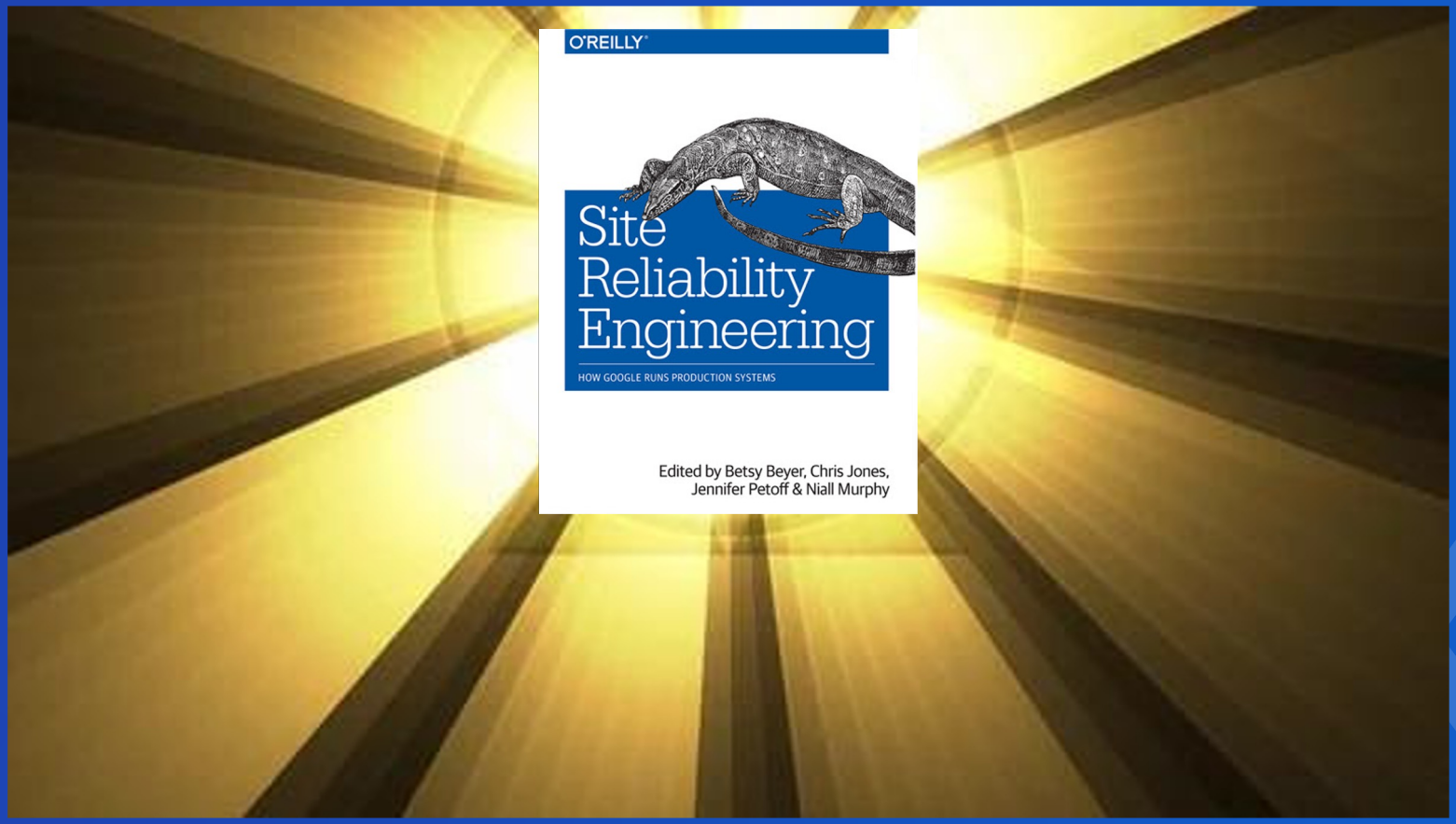
- Principal Technical Evangelist
  - ***at Kentik***
- ~35 yrs in tech.
- ~25 yrs monitoring & observability.
- ~10 yrs as a Tech Evangelist, DevRel Advocate, and (ugh) “Head Geek”.
- Tivoli, BMC, OpenView, janky perl scripts, Nagios, SolarWinds, DOS batch files, Zabbix, Grafana, New Relic, and other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

@LeonAdato on social media.

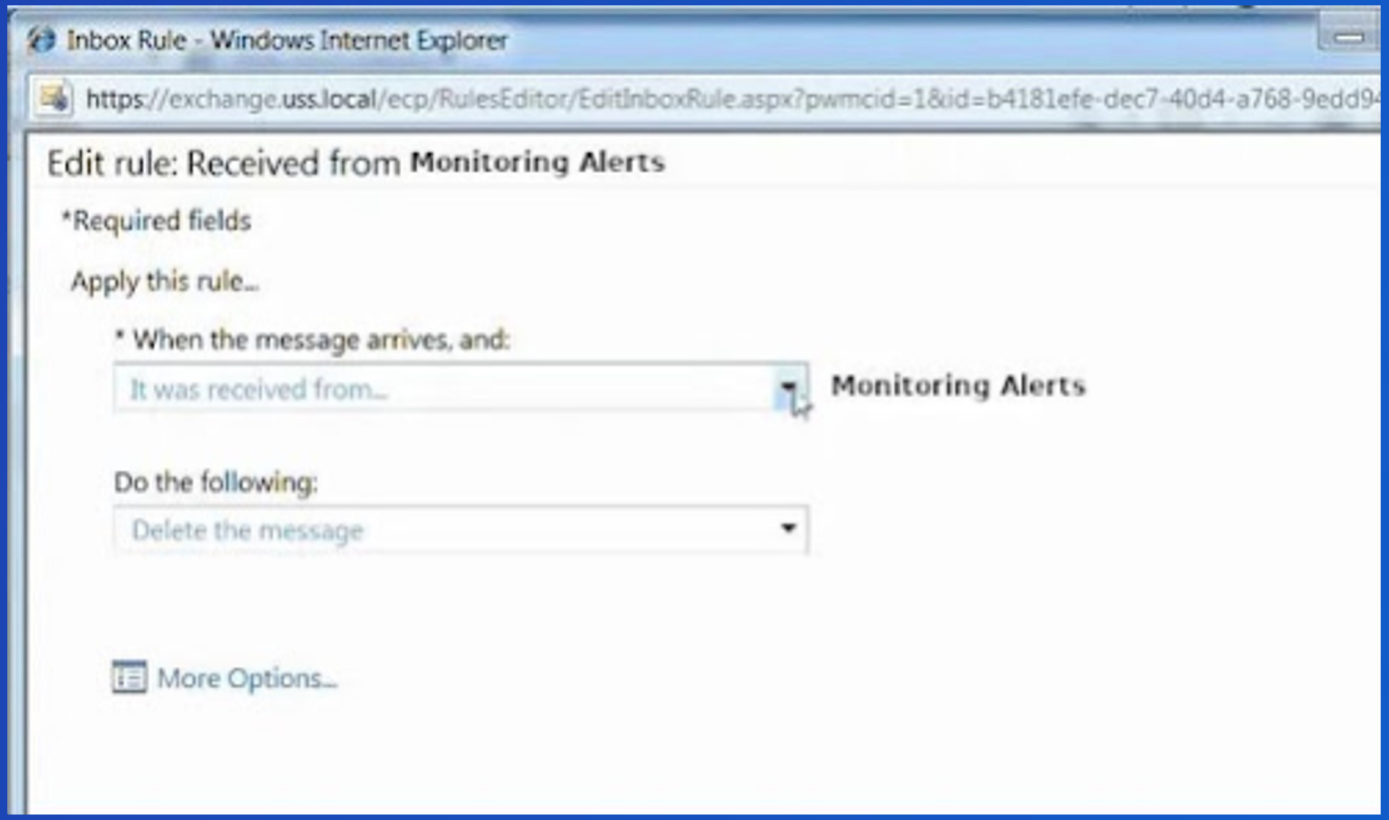
This is an Oyster Talk™

@LeonAdato

The Good Book Says....



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



** Everyone has one, and they all stink*

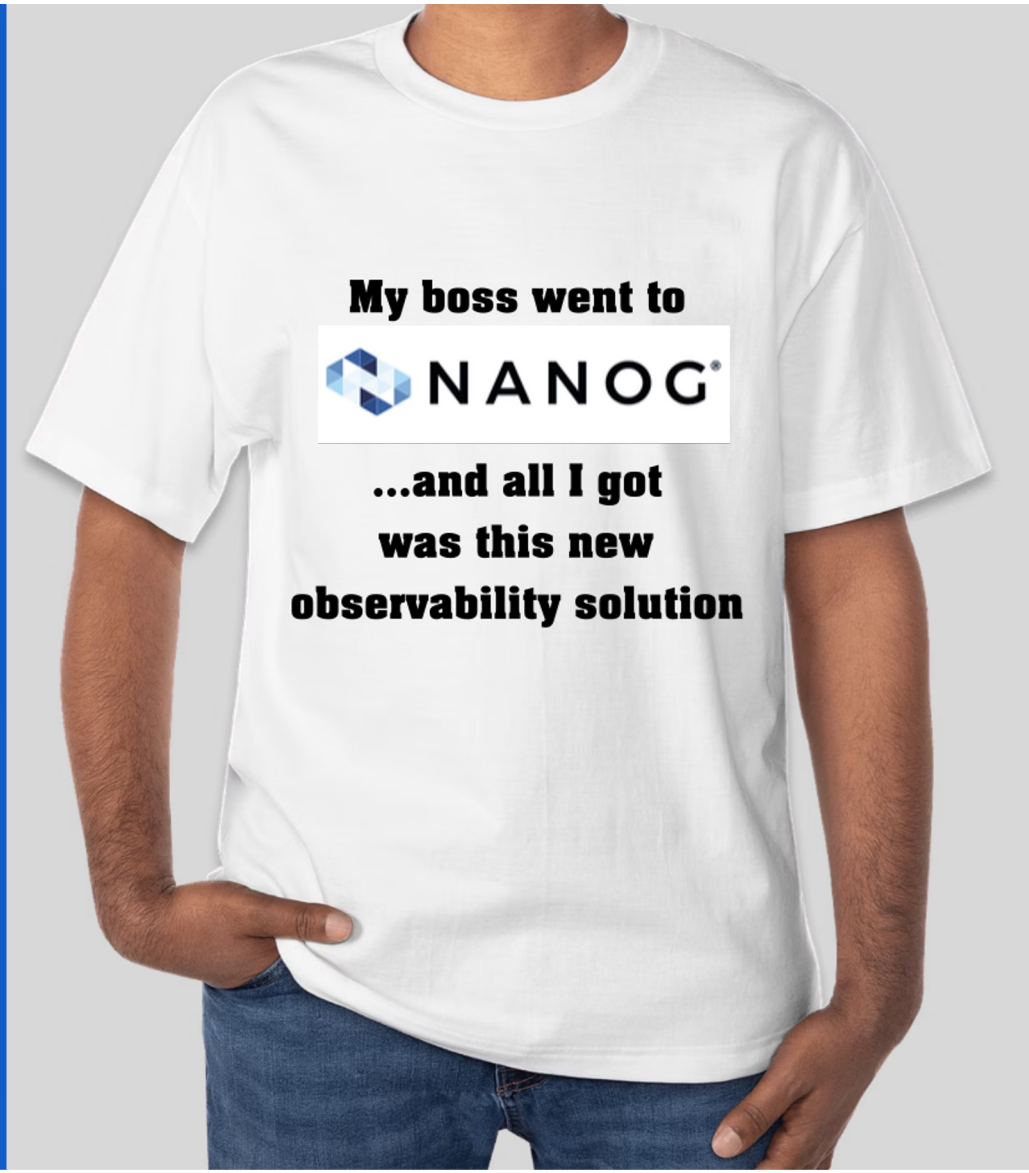
A hill I will die on

Lesson One: Alerts Are…

Three Important Rules:

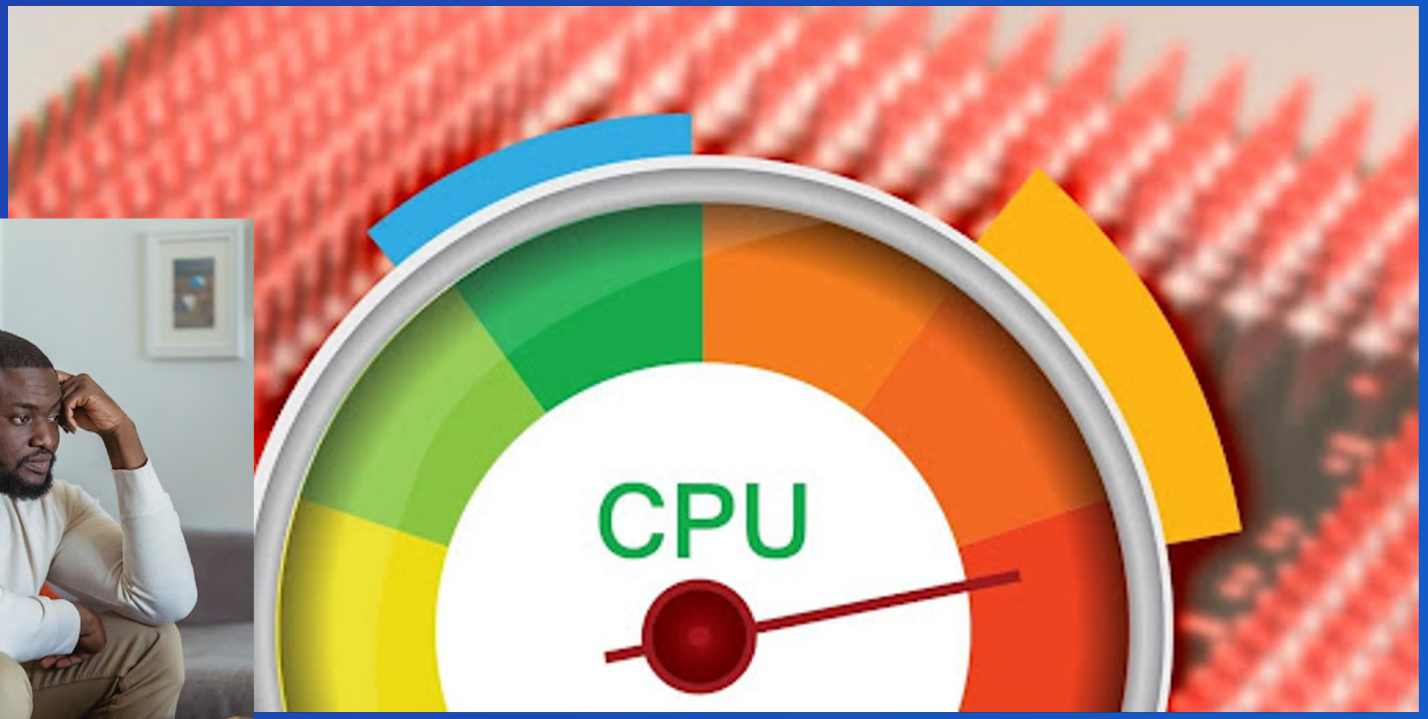
- Alerts <> Monitoring
- Alerts != Monitoring
- Alerts ≠ Monitoring

About once a year…

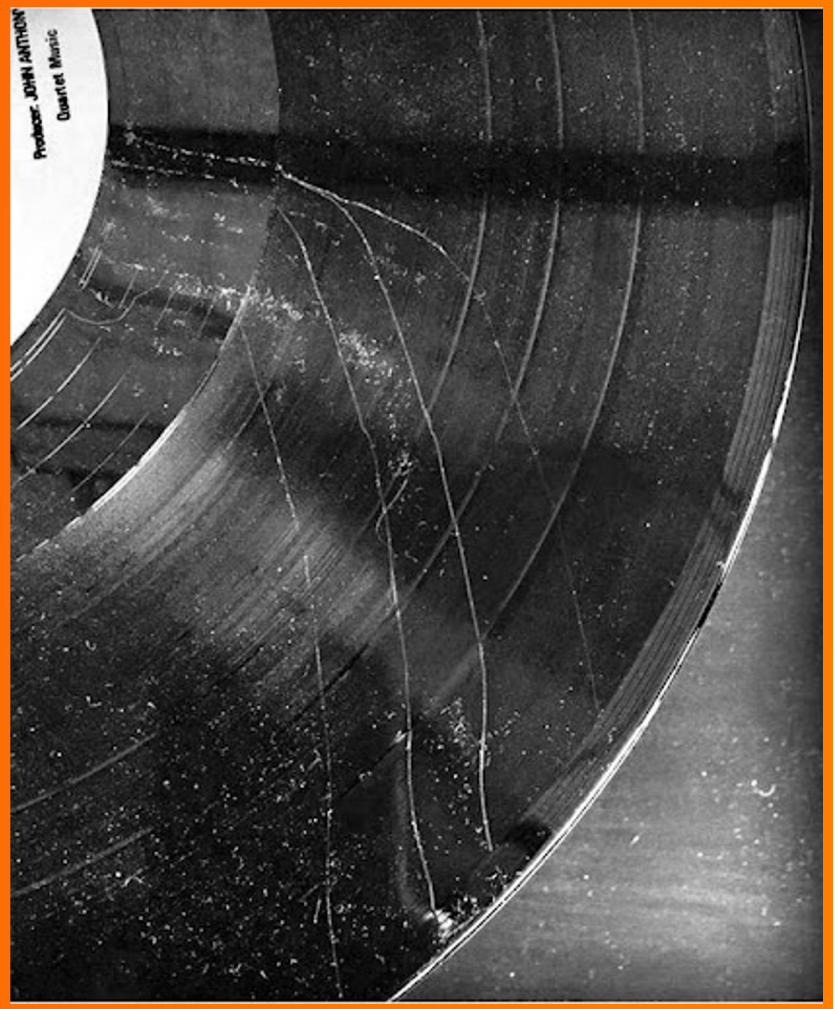


@LeonAdato

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

Monitoring

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

Alerts and Observability

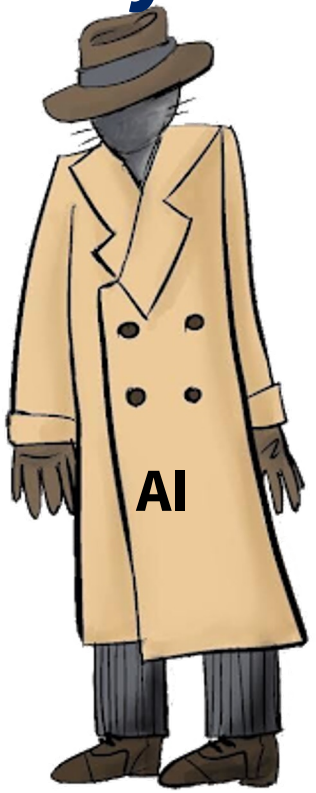
Observability

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

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

@LeonAdato

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

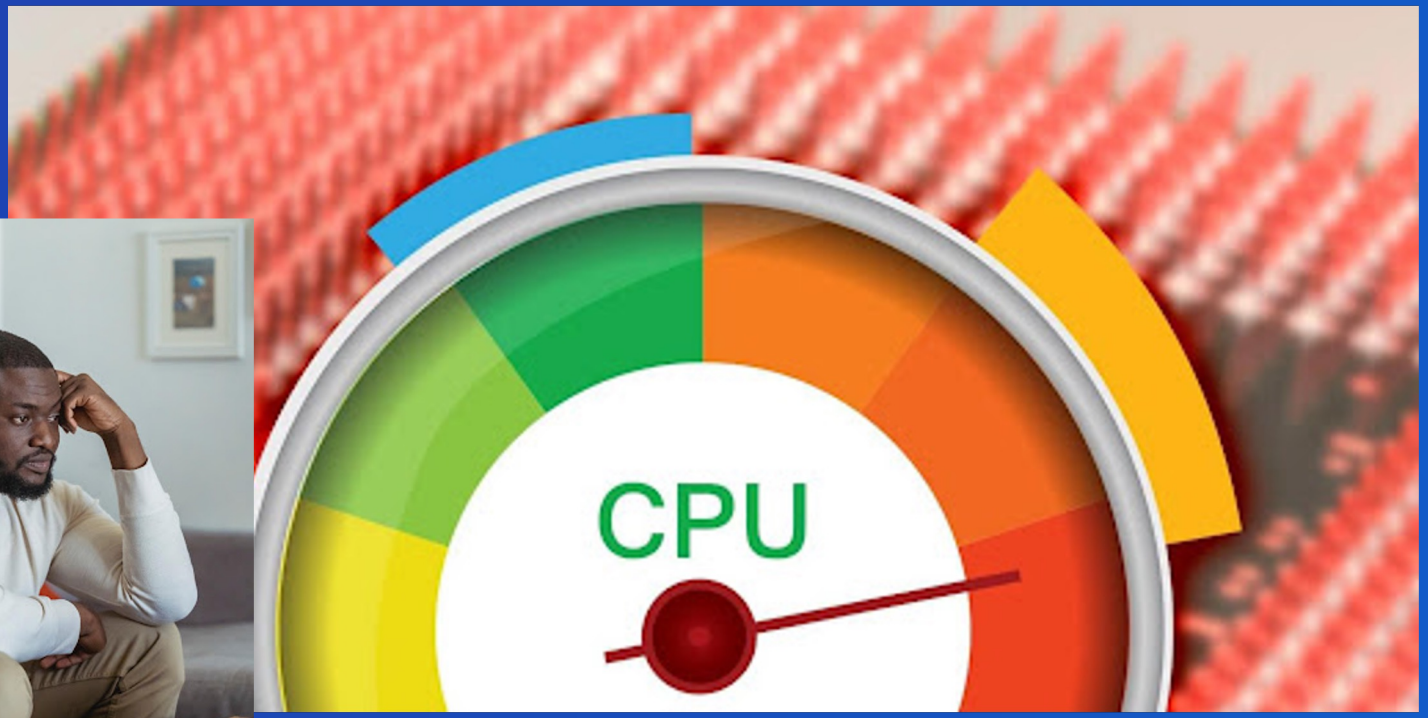
== report

== dashboard

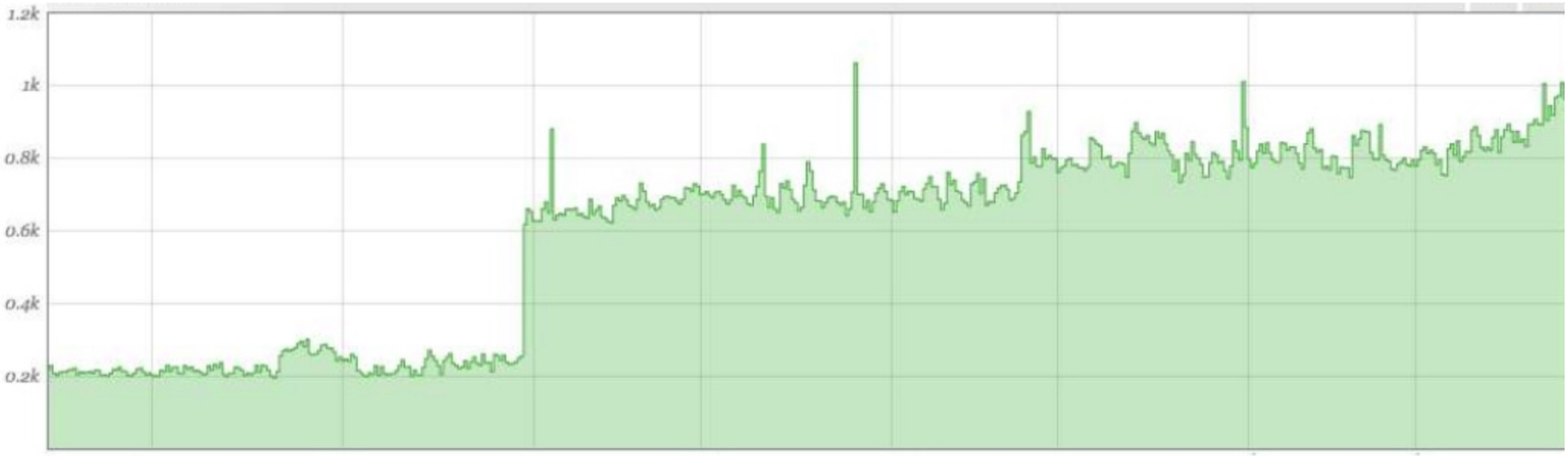
== ***Delete. It.***

@LeonAdato

The problem with high CPU alerts isn’t the CPU



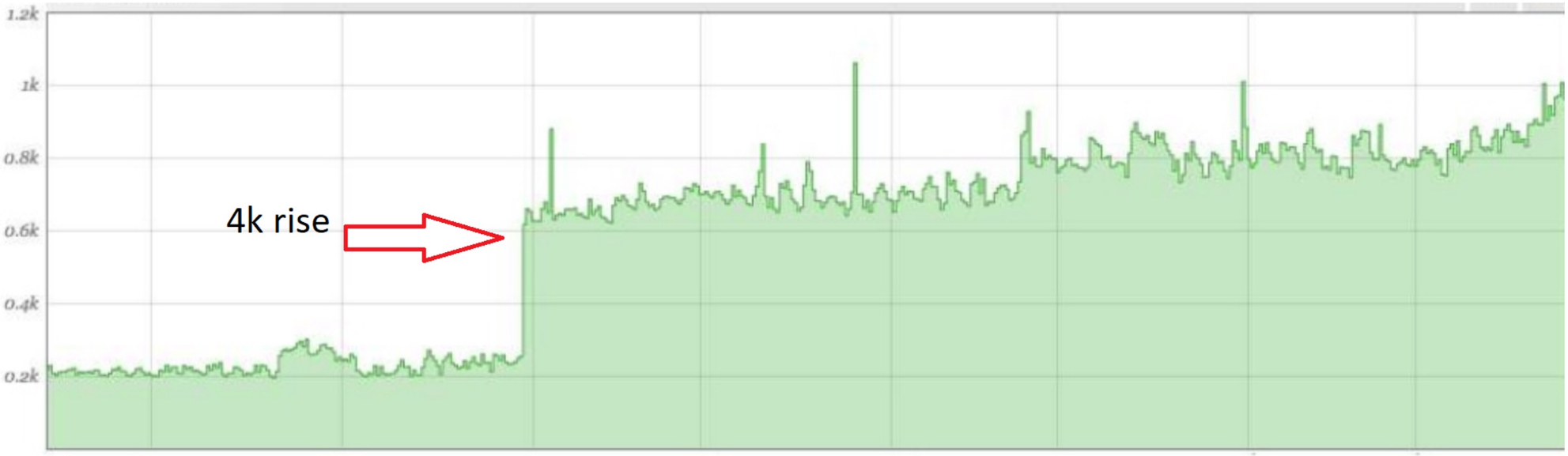
Do you see it?



Credit: Leon Fayer

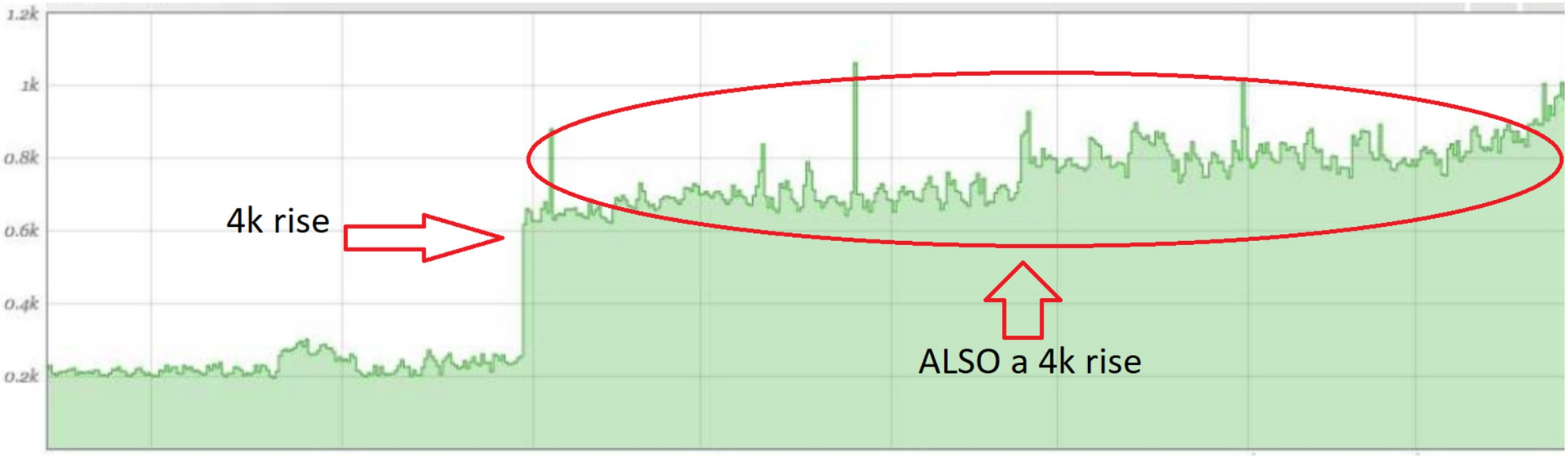
@LeonAdato

Do you see it?



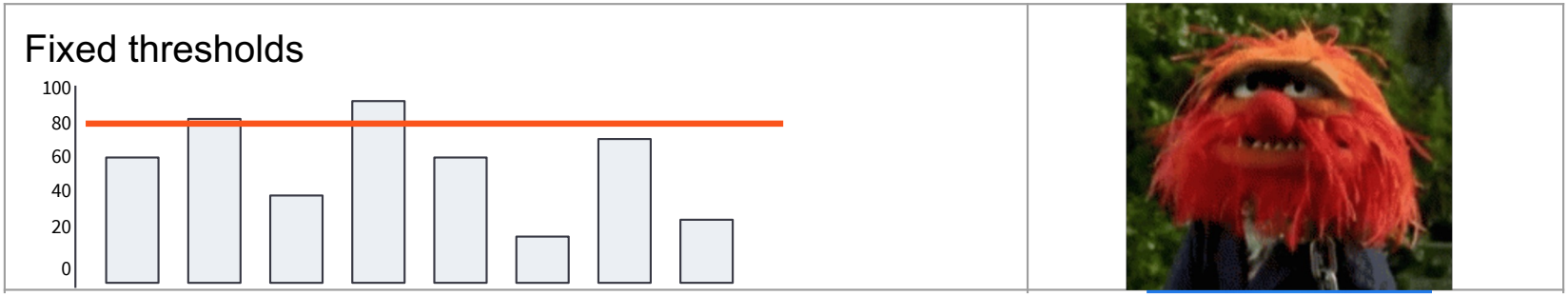
Credit: Leon Fayer

Do you see it?

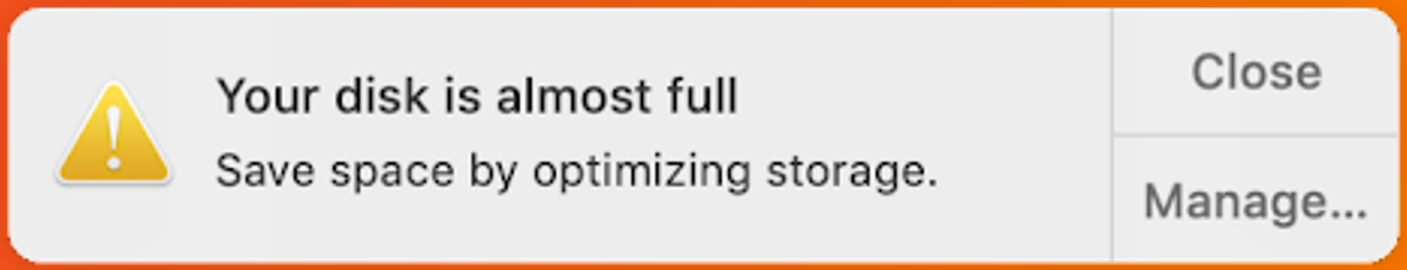


Credit: Leon Fayer

Monitoring is like Music: Both need a solid baseline!

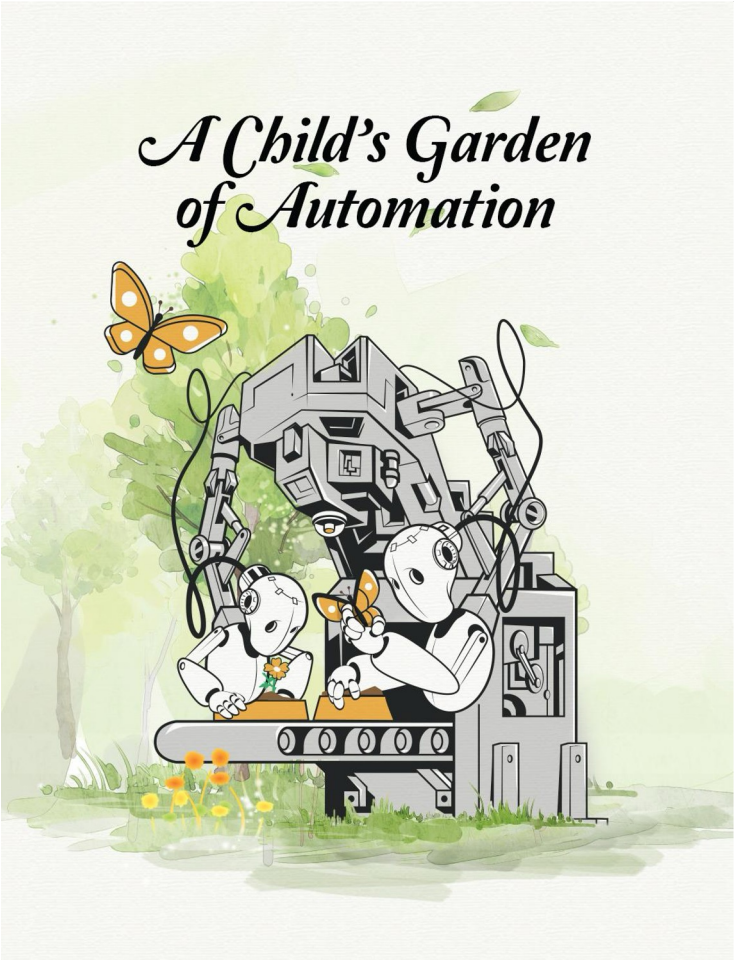


Yes, it’s a problem



But what do you DO about it?

What we have here is…
…a failure to AUTOMATE



@LeonAdato

Why Do Network Engineers Drink?

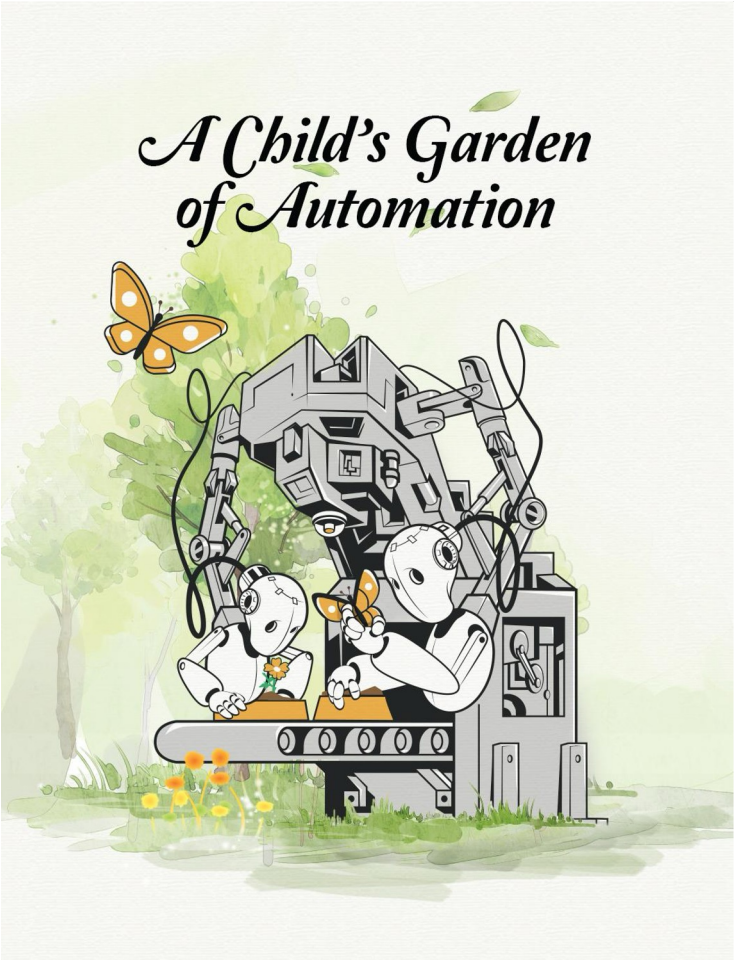
(automated) Insight

- Time to first byte vs three way handshake
- CPU/RAM on the device(s)
- ingress/egress interface info
- Path information
- Latency, packet loss, jitter
- MTU configuration
- Duplex configuration
- TAC information

What we have here is…
…a failure to AUTOMATE

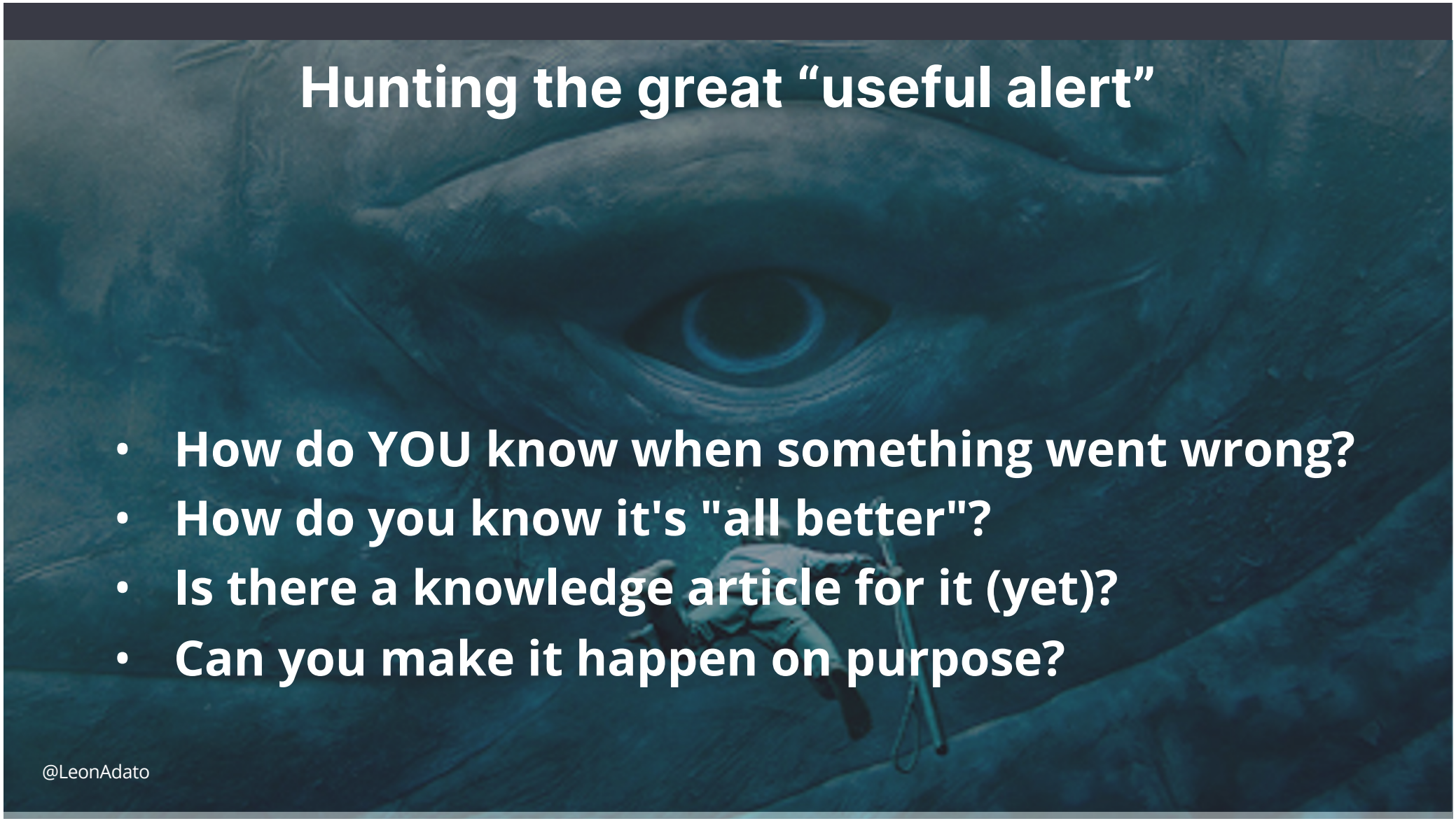
When (this thing) goes wrong,
What do YOU do about it?

@LeonAdato



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?

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

Lesson Five:
The work never ends

Ancient Wisdom

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

\- Ethics of our Fathers 2:16

Are you  ?

I’m ready for your questions!

@LeonAdato