Once Upon a Time...
Alerts don’t suck. YOUR alerts suck!

@LeonAdato
Principal Technical Evangelist

The network observability company
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

No FYI Alerts
Lesson One: Alerts Are... what?!?
Three Important Rules:

- Alerts $\not\equiv$ Monitoring
- Alerts $\neq$ Monitoring
- Alerts $\neq$ Monitoring
About once a year…

My boss went to 2024 Codemash Prime
…and all I got was this new observability solution

@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
A simple algorithm:

\[ IFF(\text{Human} \land \land \text{do something} \land \land \text{now} \land \land \text{about $problem$}) = true \]
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

@LeonAdato
Do you see it?

Credit: Leon Fayer

@LeonAdato

4k rise
Do you see it?

Credit: Leon Fayer

@LeonAdato
Monitoring is like Music: Both need a solid baseline!

Fixed thresholds

@LeonAdato
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?

@LeonAdato
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 Interrogation... 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
“Turn it over, and [again] turn it over, for all is therein.”
- Pirkei Avot (Ethics of the Fathers) 5:22

“It is not your duty to finish the work, but neither are you at liberty to neglect it.”
- Pirkei Avot 2:16
Are you *irritated*?

I’m ready for your questions!

@LeonAdato