

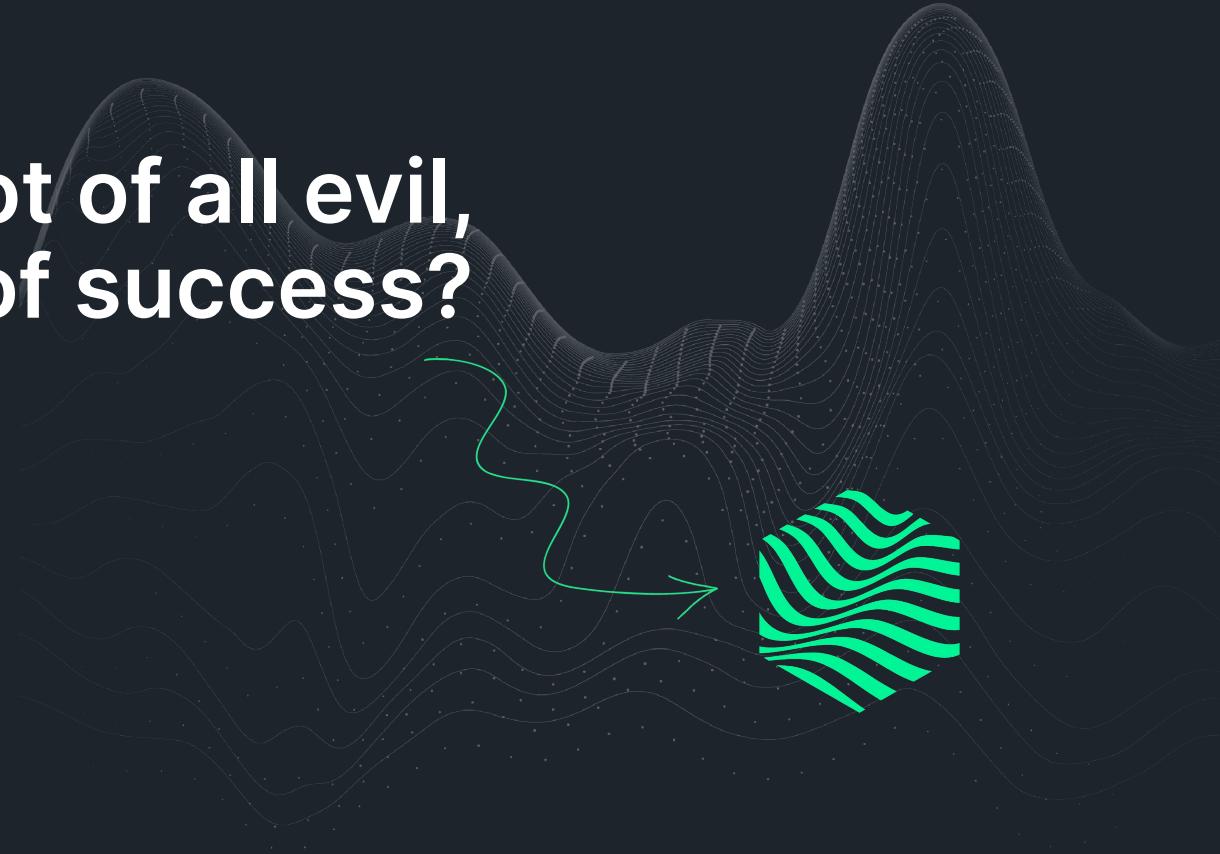
Once Upon a Time...



Alerts: the root of all evil, or the seeds of success?

@LeonAdato

\$date();





Leon Adato

- Principal DevRel Advocate @ New Relic
- Started in tech ~33 yrs ago
- Focus on monitoring for ~20 yrs
- Tivoli, BMC, OpenView, Nagios, SolarWinds
Perl scripts, batch files,
and New Relic (duh)
- Built monitoring for small, medium,
and ludicrous size orgs.
- @LeonAdato almost everywhere

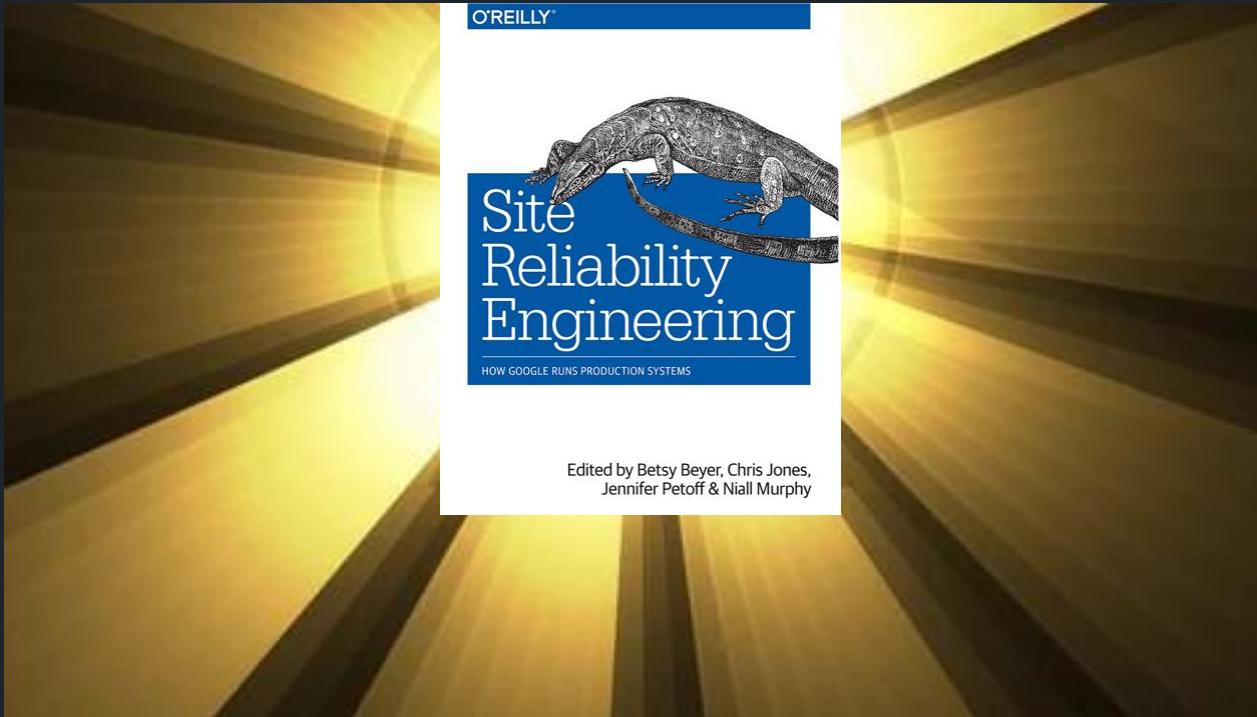
This is an Oyster Talk™



@LeonAdato

 new relic

The Good Book Says...



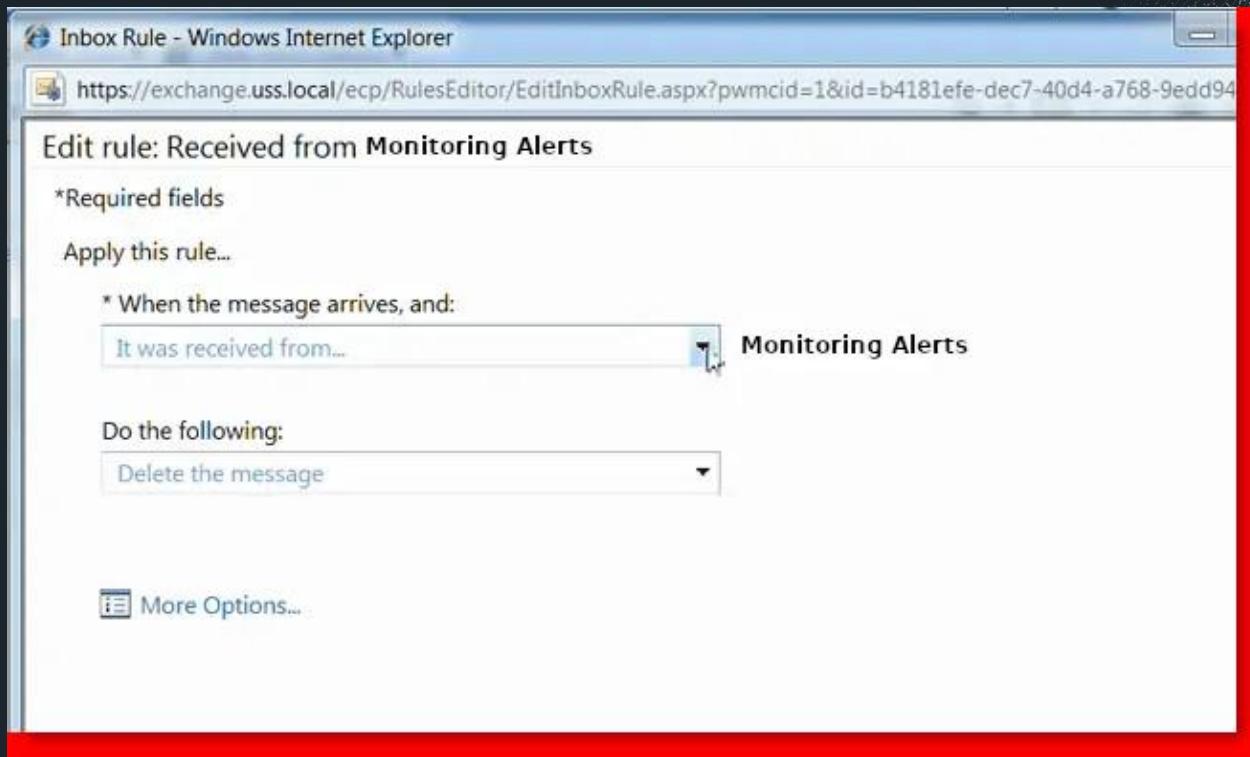
@LeonAdato



Lesson One: Alerts Must Matter



Inbox Rules are like a\$\$holes...

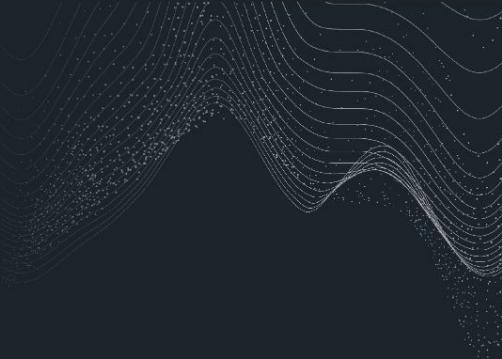


The hill I will die on



@LeonAdato

A simple algorithm



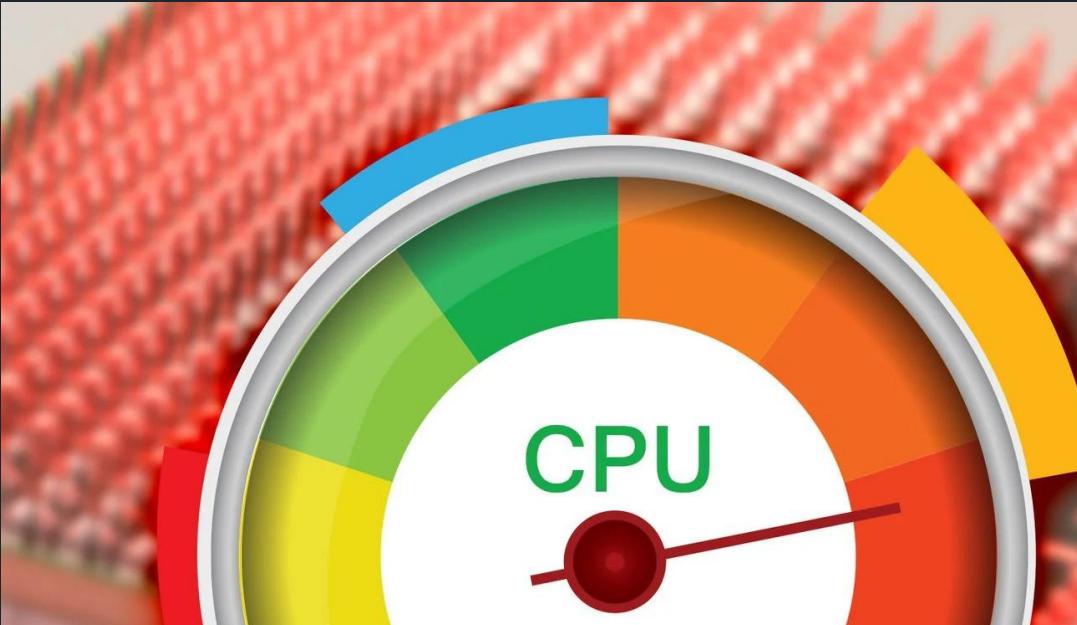
IFF(Human && do something && now && about \$problem) == true

If it's not an alert, what is it?

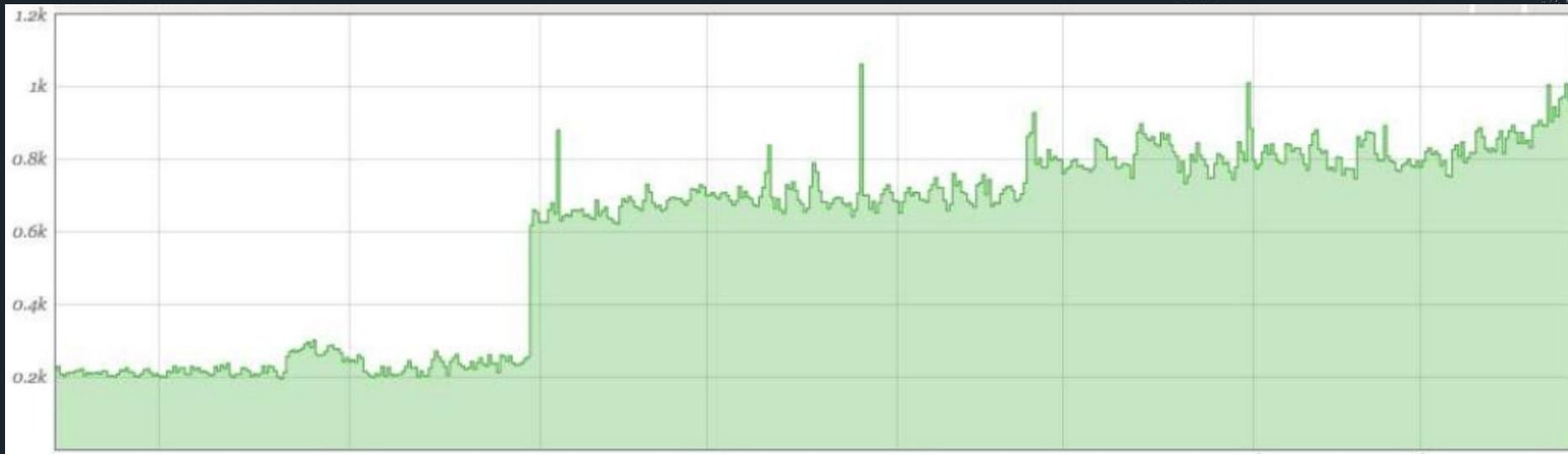
IFF (Human && do something && now && about \$problem) == true

- (!= human) == automation
- (!= now) == report
- (!= problem) == dashboard
- (!= doing something) == delete

The problem with high CPU alerts isn't the CPU



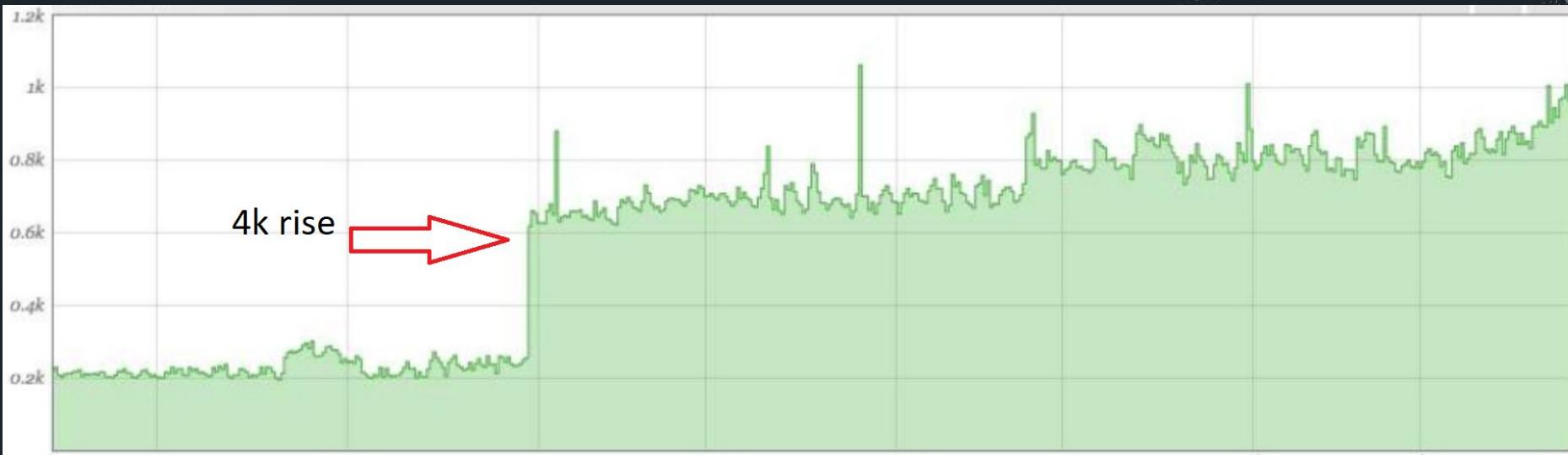
Do you see it?



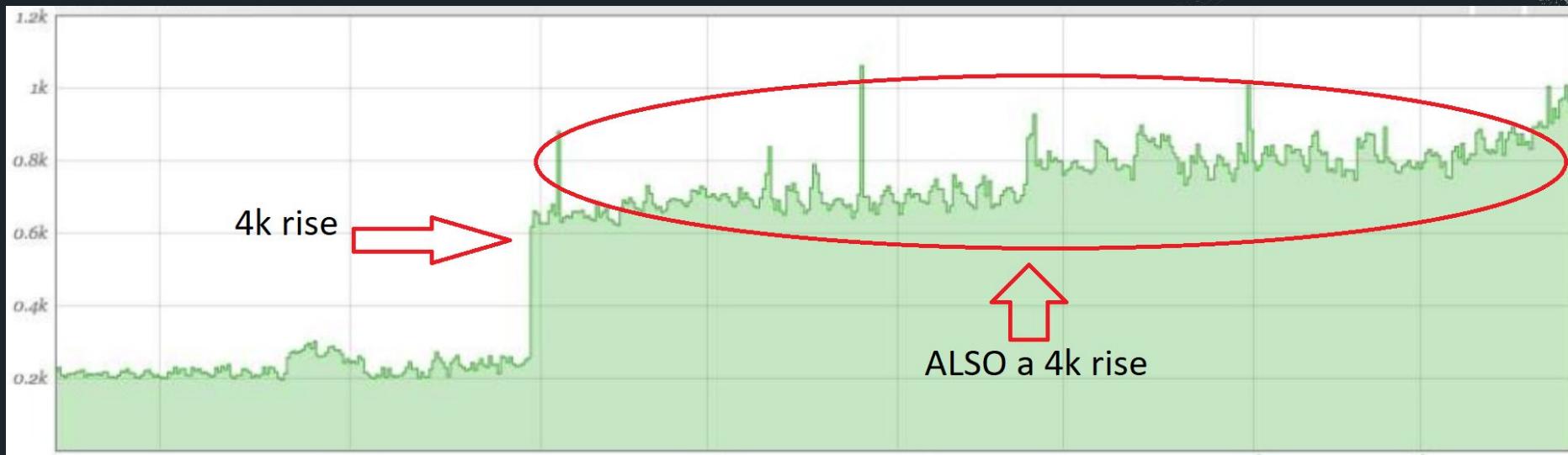
@LeonAdato



Do you see it?



Do you see it?



Monitoring

&&

Observability



LESSON 2: Skilled Interrogati... Interviewing



@LeonAdato

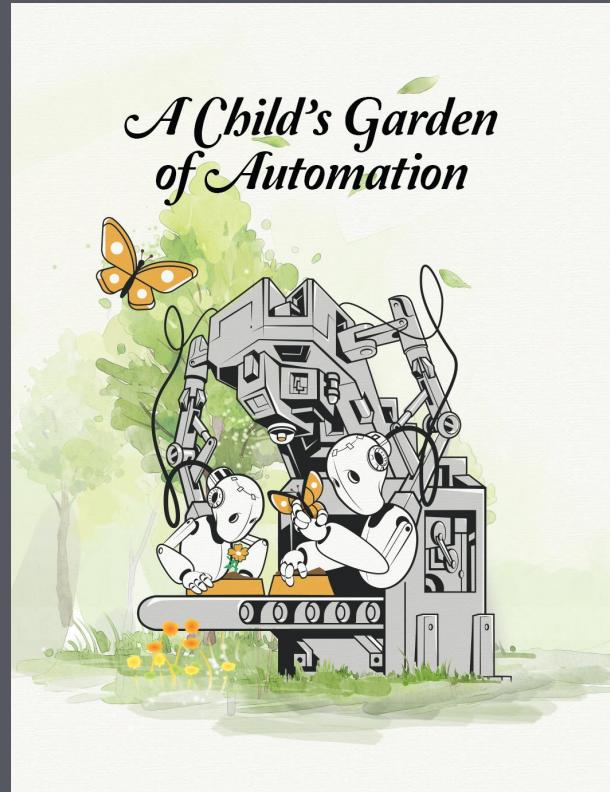
 new relic

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 see one happen in the wild.

LESSON 3: Automation, not Art

“When something goes wrong,
what do YOU do about it?”



@LeonAdato

 new relic

The GEPHRINKEL command?!?



@LeonAdato

 new relic

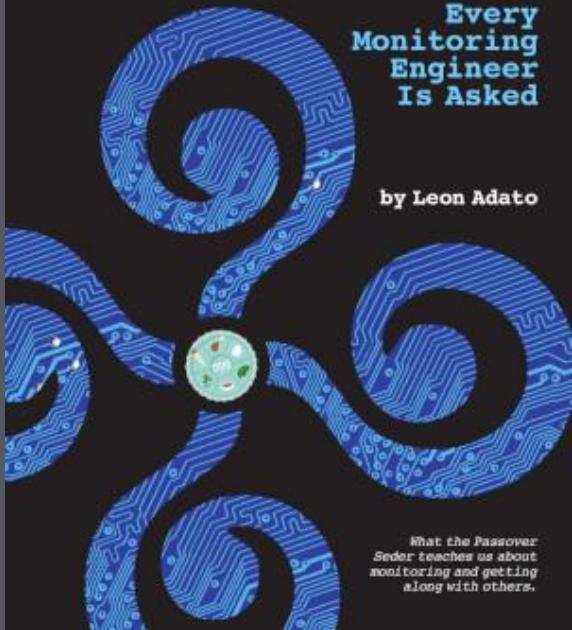
Shared responsibility model -- THEY OWN IT



@LeonAdato

 new relic

The Four Questions



LESSON 4: The Four Questions

Question 1: Why Did I Get This Alert?



“Your system is down”



Closed Sales on the Windows service owned by Sales named Close_Rate (IP: 10.2.3.4, DNS: CART..MyCorp.Net) has been under 80% for more than 15 minutes. Closes at 2:16am EST is 56%. Device details: <http://blahblah>. Acknowledge this alert: <http://ackme> This message brought to you by the alert: CLOSE_CRIT_PROD and the polling engine Poller7

@LeonAdato

new relic

Question 2: Why DIDN'T I get an alert?

- It was designed like that
- Change UN-control
- Monitoring failed

@LeonAdato



Question 3: What is being monitored on my stuff?

nodeid	caption	LED	elementtype	element	Description	capacity	threshold	value	warn	crit
1	stp-aix71	Up.gif	CPU	CPU Count:		4	0	CPU Utilization	80	90
1	stp-aix71	Up.gif	RAM	Total RAM		8.32E+09	0	RAM Utilization	80	90
1	stp-aix71	Up.gif	NIC	ent1	Ethernet	1000000000	bandwidth in/out	80/80	90/90	
1	stp-aix71	Up.gif	DISK	/dev/fwdump	Fixed Disk	134217728				
4	VMAN-2008R2-IIS.vman.lab	Up.gif	CPU	CPU Count:		2	0	CPU Utilization	80	90
4	VMAN-2008R2-IIS.vman.lab	Up.gif	RAM	Total RAM		2.15E+09	0	RAM Utilization	80	90
4	VMAN-2008R2-IIS.vman.lab	Up.gif	NIC	Intel(R) PRO/1000 MT Network Connection	Ethernet	1000000000	bandwidth in/out	80/80	90/90	
4	VMAN-2008R2-IIS.vman.lab	Up.gif	DISK	C:\ Label: 583721ff	Fixed Disk	42842714112				
4	VMAN-2008R2-IIS.vman.lab	Unknown	APP	Processor Queue Length	01LJA_Windows_Standard		0	CPU Utilization	NULL	NULL
8	LAB-NLB2012-02	Up.gif	CPU	CPU Count:		2	0	CPU Utilization	80	90
8	LAB-NLB2012-02	Up.gif	RAM	Total RAM		2.97E+09	0	RAM Utilization	80	90
8	LAB-NLB2012-02	Up.gif	NIC	Microsoft Hyper-V Network Adapter	Ethernet	1000000000	bandwidth in/out	80/80	90/90	
8	LAB-NLB2012-02	Up.gif	DISK	C:\ Label: EEBFA16E	Fixed Disk	42579521536				
8	LAB-NLB2012-02	Up	APP	Processor Queue Length	01LJA_Windows_Standard		0	CPU Utilization	NULL	NULL
10	Tex-3750.aus.lab	Up.gif	CPU	CPU Count:		1	0	CPU Utilization	80	90
10	Tex-3750.aus.lab	Up.gif	RAM	Total RAM		1.33E+08	0	RAM Utilization	80	90
10	Tex-3750.aus.lab	Up.gif	NIC	GigabitEthernet0/0	Ethernet	1000000000	bandwidth in/out	80/80	90/90	
10	Tex-3750.aus.lab	Up	HW	CISCO2821	Fan (Up): Fan 1 (Up), Fan 2 (Up), Fan 3 (Up)					
11	lab-mpls-pe-tex.lab.ew	Up.gif	CPU	CPU Count:		1	0	CPU Utilization	80	90
11	lab-mpls-pe-tex.lab.ew	Up.gif	RAM	Total RAM		7.11E+08	0	RAM Utilization	80	90
11	lab-mpls-pe-tex.lab.ew	Up.gif	NIC	FastEthernet0/0	Ethernet	100000000	bandwidth in/out	80/80	90/90	
11	lab-mpls-pe-tex.lab.ew	Up.gif	NIC	FastEthernet0/0-mpls layer	MPLS	100000000	bandwidth in/out	80/80	90/90	
11	lab-mpls-pe-tex.lab.ew	Up.gif	NIC	FastEthernet0/1	Ethernet	100000000	bandwidth in/out	80/80	90/90	
11	lab-mpls-pe-tex.lab.ew	Up	HW	CISCO2811	Fan (Up): Fan 1 (Up), Fan 2 (Up), Fan 3 (Up)					

@LeonAdato

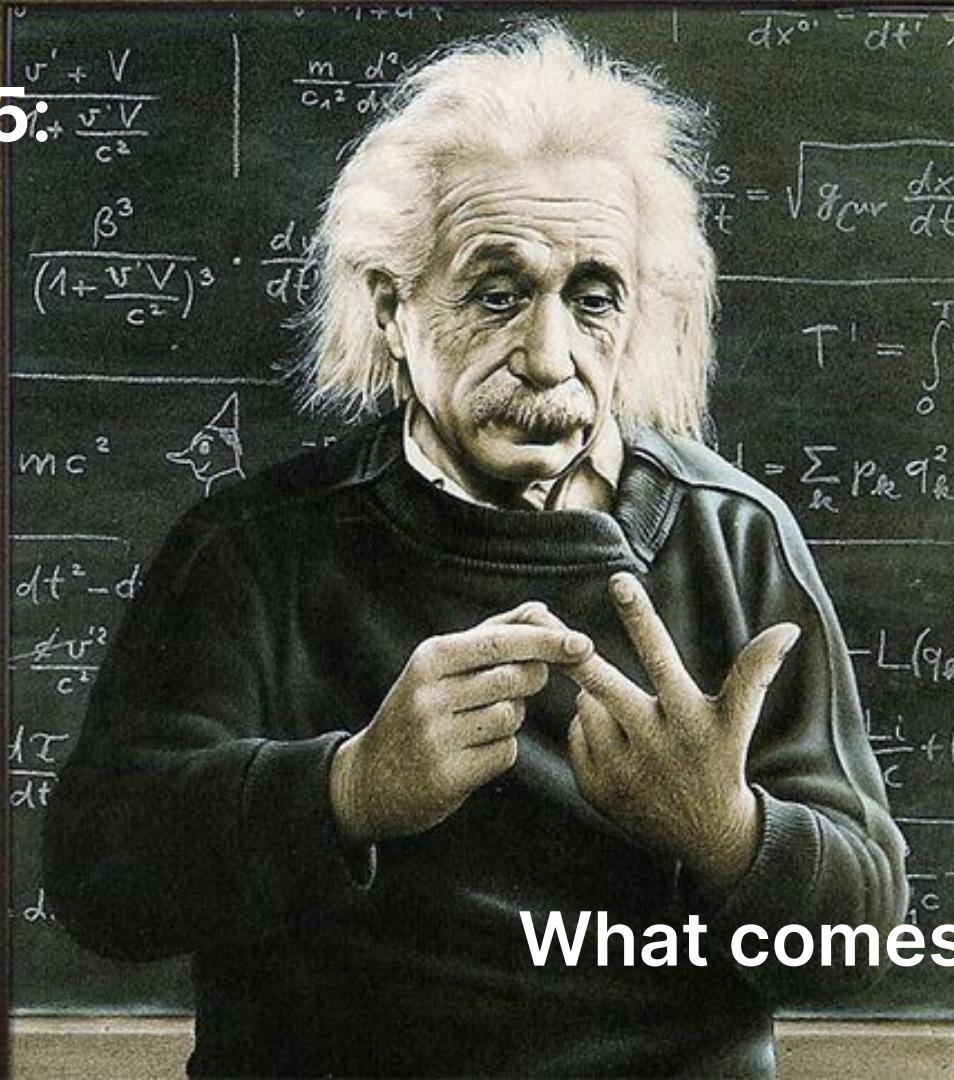
Question 4: What alerts could MY stuff trigger?

- What *IS* an alert?
 - Emergency
 - Interruption
 - Unplanned Work
- What does alerting NEED to be
 - Timely
 - Meaningful
 - Actionable

@LeonAdato



Question 5:



What comes “standard”?

Question 5: What comes “standard”?

- When you load up a <thing> into your solution, what do consumers automatically get?
- If you can't describe this, how will anyone know what to ask for “extra”?

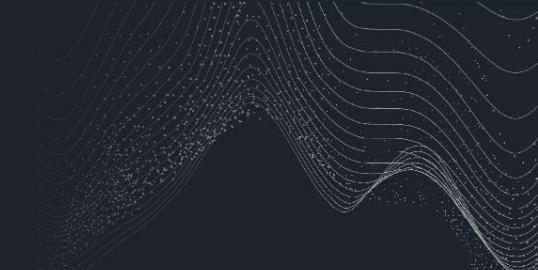
@LeonAdato



LESSON 5:

The Work Never Ends





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

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

**לֹא עַלְיךָ הַמְלָאכָה לִגְמֹר
וְלֹא אַתָּה בֶּן חֹרֵין לְבַטֵּל מִמְפָנָה**

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

- Pirkei Avot 2:16

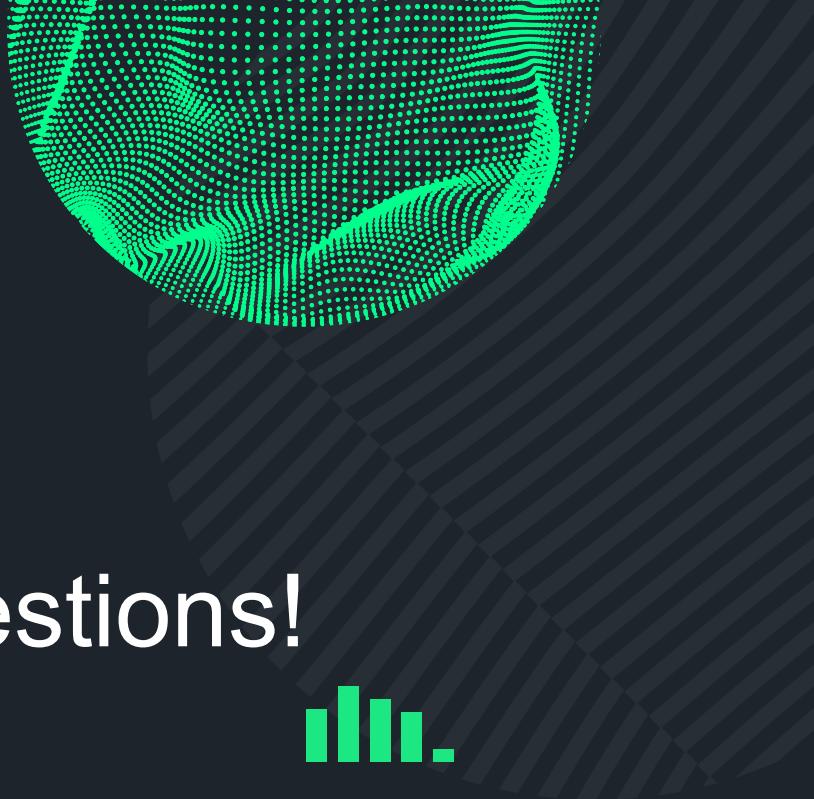
@LeonAdato

 new relic

מה פתקאות



Irritated?



I'm ready for your questions!



@LeonAdato