Incident Response

One Thing

Shaun Mouton

Tirefi.re, Friendgineering Directorate

Ops, sometimes
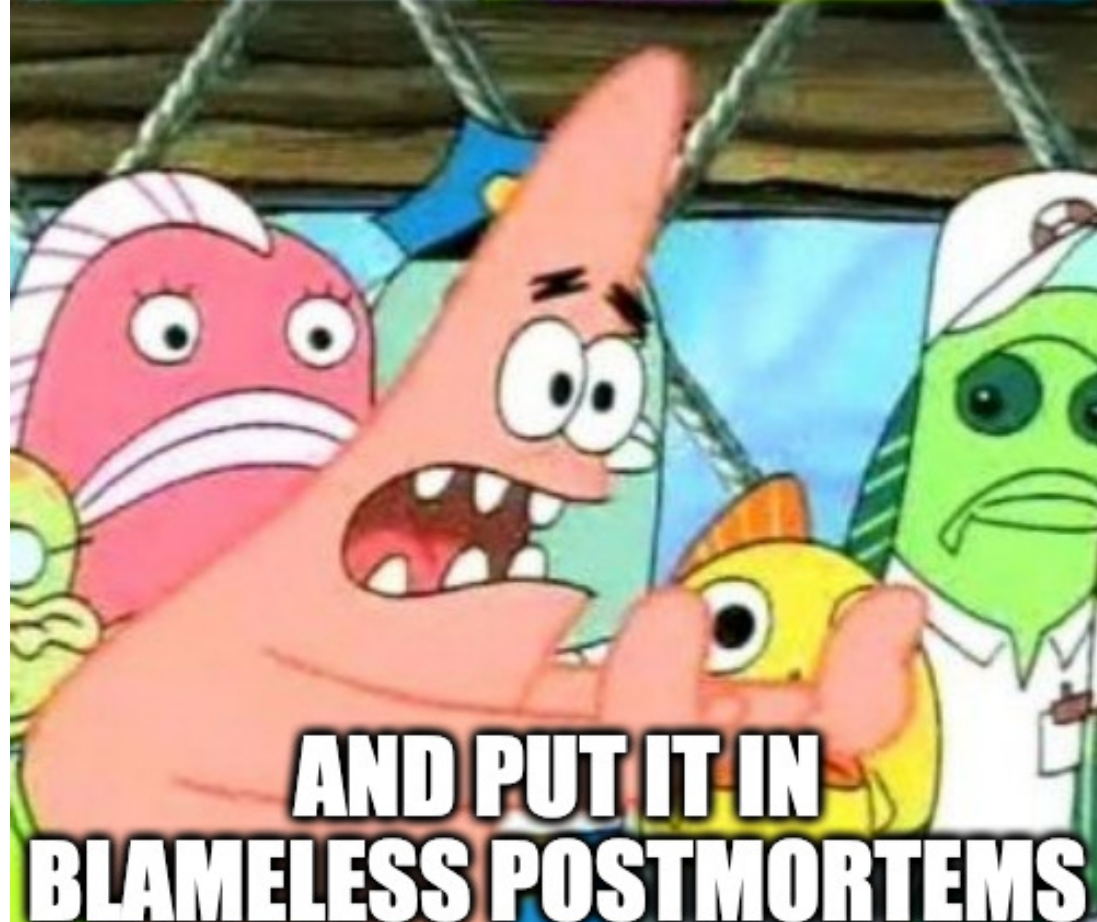
Incident Response

the old good way

thanks for everything

John Allspaw and crew, of Etsy

Incident Response Response

the new old way

thanks for everything

people who didn't read what Allspaw & co.
wrote

or listen to what they said

Incident Response Response Response

the new new way

thanks for everything

Allspaw, Sidney Dekker & the Lund U. Crew

<3 J Paul Reed

See Also, These Things

Karl Katzke's Austin Devops talk about incident response at Kasasa

Boyd Hemphill's talks about workflows at Contrast Security

An Update From The Field

OH: holy shit incident command with indignant engineers is wild style!!!!!1

The Gritty

I leave Chef this month after nearly 4 years

I have worked at least 75 Severity 1 incidents for in that time, mostly for F100 enterprises.

(more than 75 less than 380, our tracking for who worked what could have been better)

The Gritty, Nitty

3/4 of the people who've reached out to me have commented about my ability to remain cool under pressure.

I have heard something similar from folks in previous jobs

I do not think you have to be a chonky white dude to have folks appreciate your value in a crisis.

Incident Response To-Do List 1

Chill Out.

If you're gonna lose your job due to this, you can find a less stressful job elsewhere.

Incident Response To-Do List 2

Calm Down.

There are enough people panicking already.

Incident Response To-Do List 3

Be Reasonable.

If nobody's able to run through the "is it plugged in? what does the error log actually say? do I need to go peepee?" list at least once an hour folks will be wasting effort and burning themselves out.

Incident Response To-Do List 4

Hand it Off.

If you have an idea and need to dig into something, make sure that someone's stepping into the "adult in the room" role, even if it's not the person everyone thinks is the incident commander.

Incident Response Mantra

I will not improve this situation by giving in to a panic response

That's It

Never half-ass two things. Whole ass one thing.