

SHIFTING LEFT SECURELY

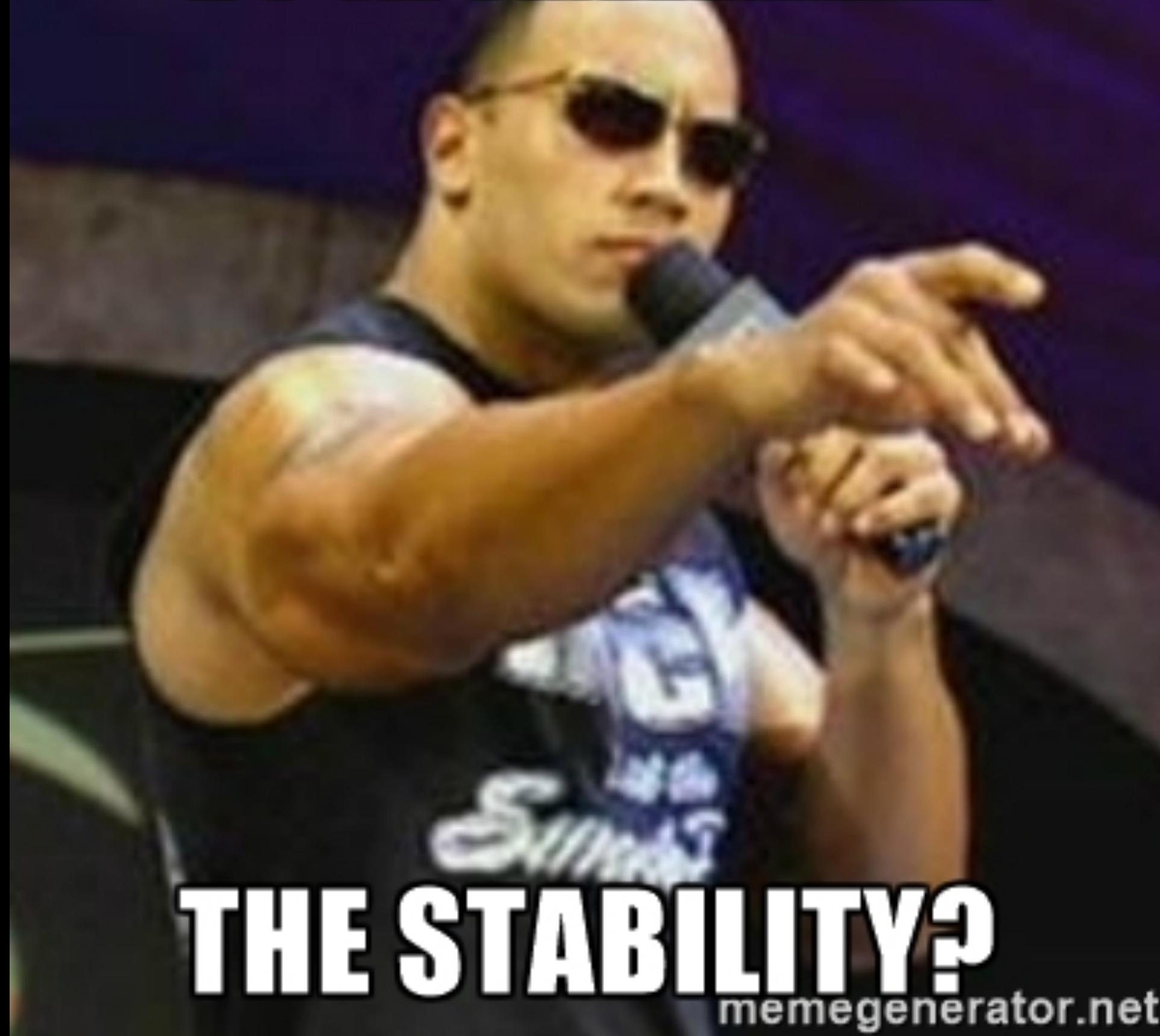
WHOAMI



@mattstratton

@MATTSTRATTON

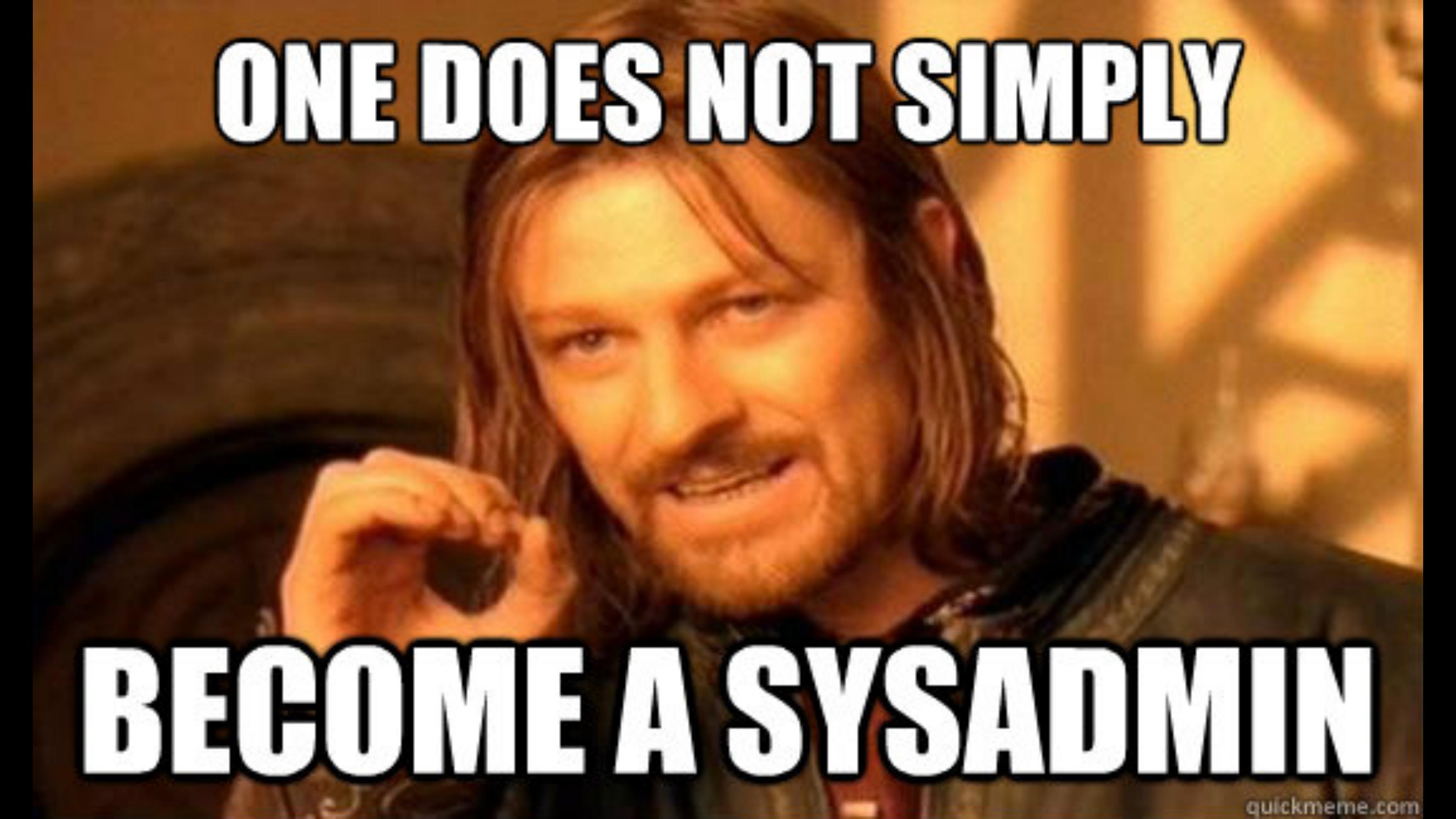
DO YA SMEELLLL



THE STABILITY?

memegenerator.net

ONE DOES NOT SIMPLY

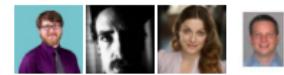
A close-up photograph of a man with long, light brown hair and a full, dark beard. He is wearing a dark leather vest over a light-colored shirt. He is holding a black handgun in his right hand, pointing it towards the camera. His left hand is resting on his chin, supporting his head. He has a serious, intense expression on his face. The background is blurred, showing what appears to be an indoor setting with warm lighting.

BECOME A SYSADMIN

Skills & Endorsements

Top Skills

4 Chef



Infrastructure As Code

7 Configuration Management



5 DevOps



2 Karaoke



Continuous Delivery

99+ Cloud Computing



2 Windows Azure



1 Amazon EC2



56 Windows Server



Matt also knows about...

28 Linux

68 IIS

74 Agile Methodologies

49 VMware

14 Hyper-V

13 Server Administration

28 Microsoft SQL Server

31 IT Operations

14 IT Service Management

19 Powershell

24 Virtualization

9 Automation

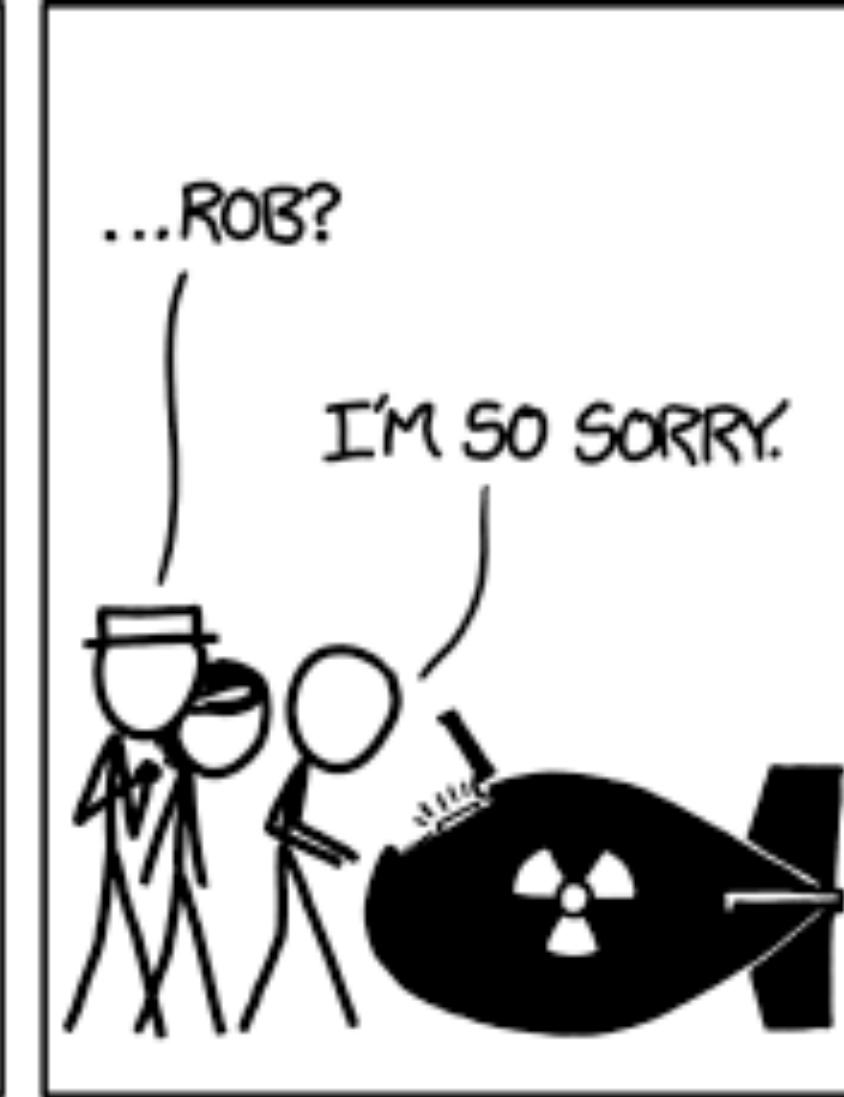
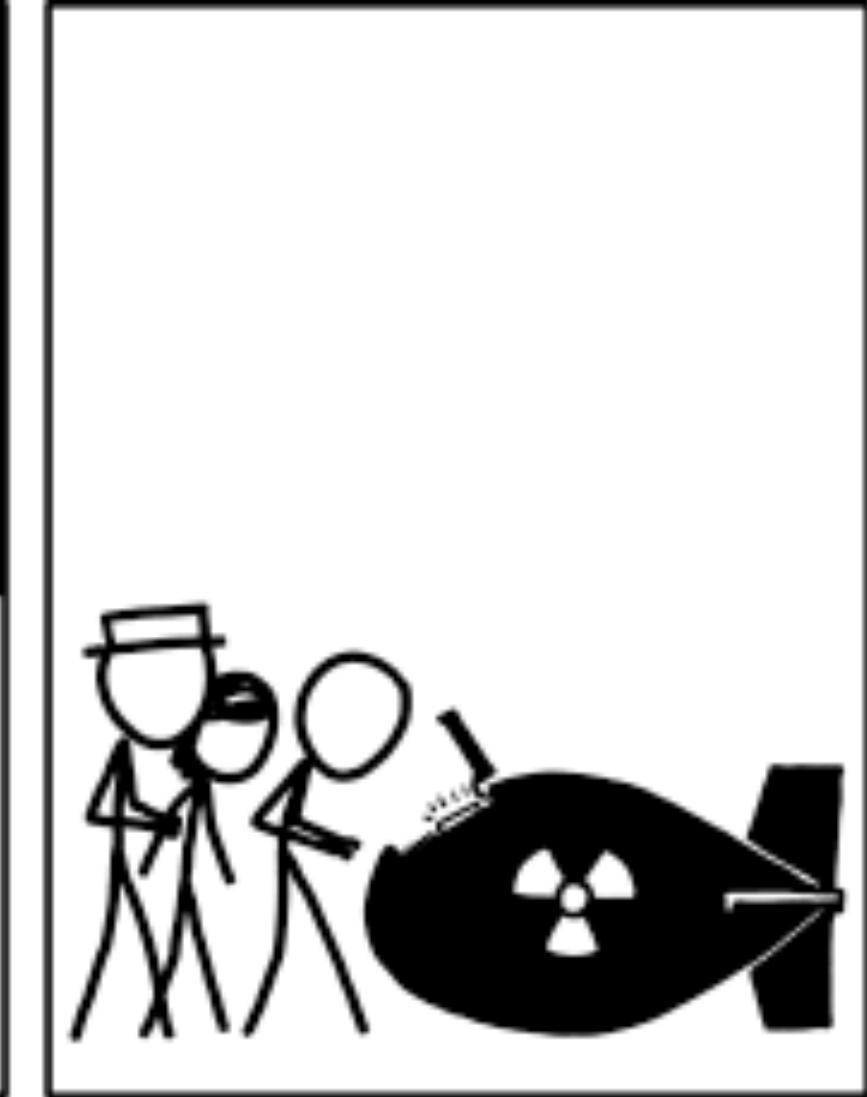
9 Microsoft Technologies

18 Data Center

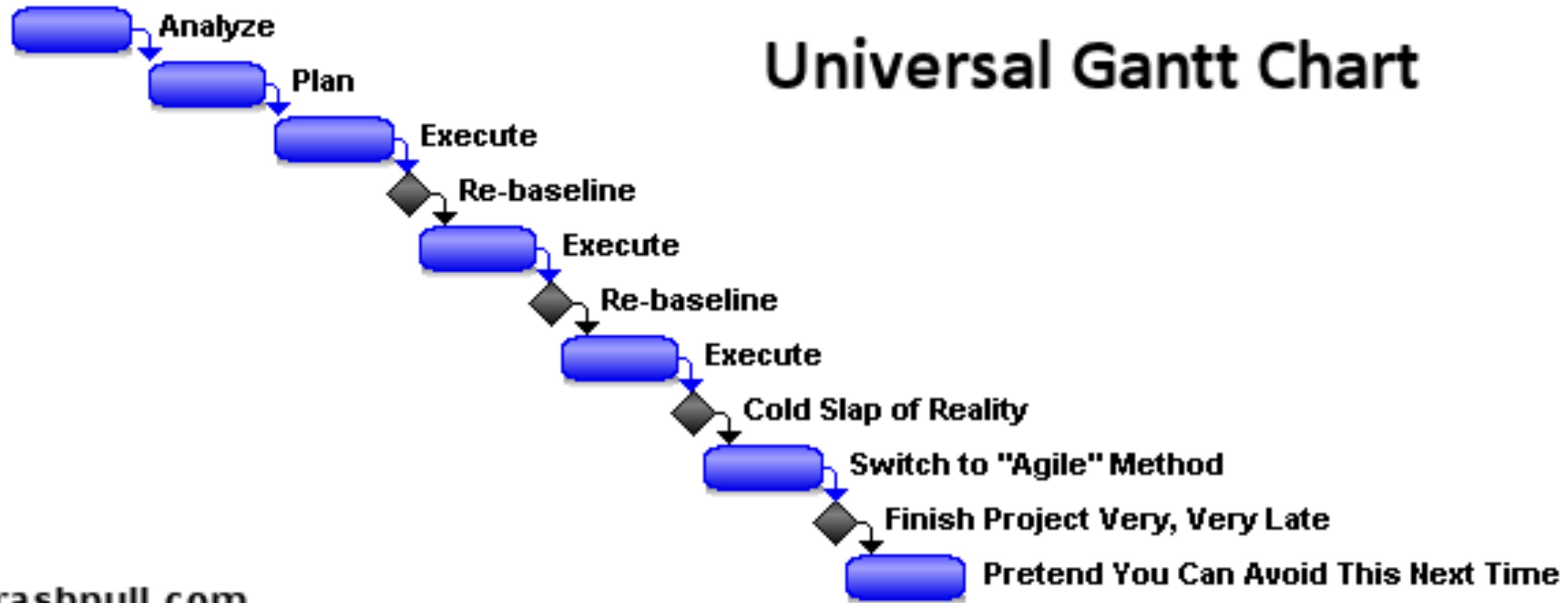
5 Release Management

A close-up shot of a man with short brown hair, wearing a light-colored button-down shirt. He is holding a black smartphone to his right ear with his right hand, looking slightly upwards and to his left with a serious expression. The background shows a wall with a framed picture of a palm tree and a window with vertical blinds.

- I'VE MADE A HUGE MISTAKE.



Universal Gantt Chart





EPIC FAIL .COM

NOT SURE IF SHIFTING

LEFT

**OR JUST DOING LESS
TESTING**

MY TESTS DIDN'T PASS



**SO I CHANGED THE
TESTS**

I DON'T ALWAYS USE A
PIPELINE



HOW DOES THIS HELP
ME WITH SECURITY?

WHAT IF WE CONTINUOUSLY TESTED FOR SECURITY

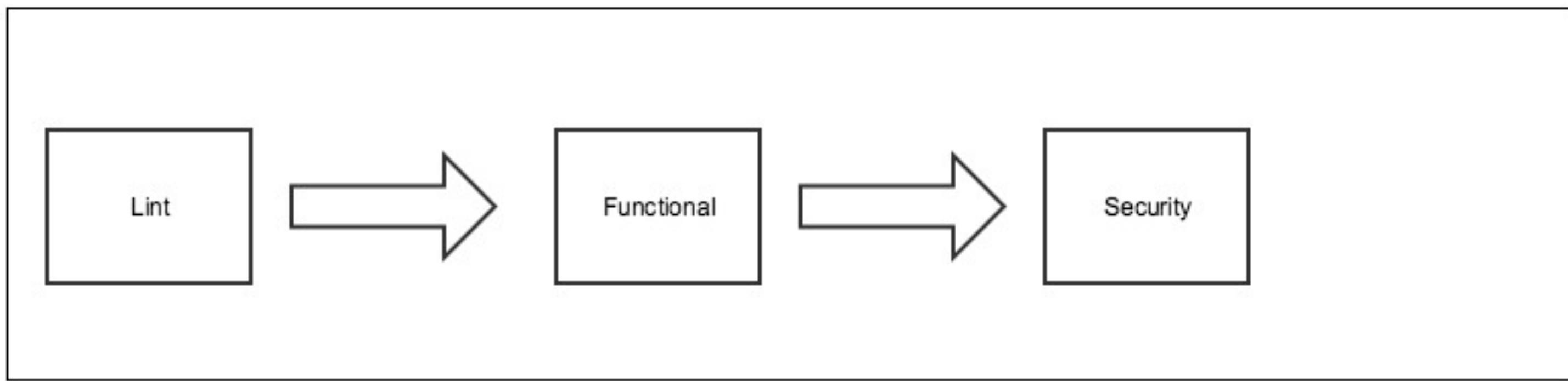


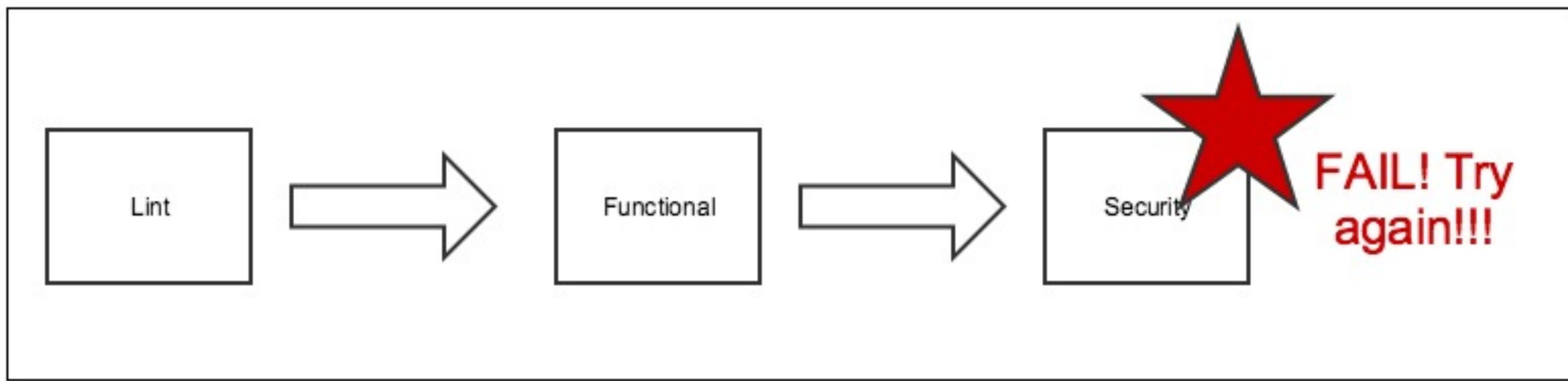
INSTEAD OF WAITING FOR A "HARDENING SPRINT"?

YOU HAVE TESTS IN THE PIPELINE



THAT I CANNOT RUN
LOCALLY?

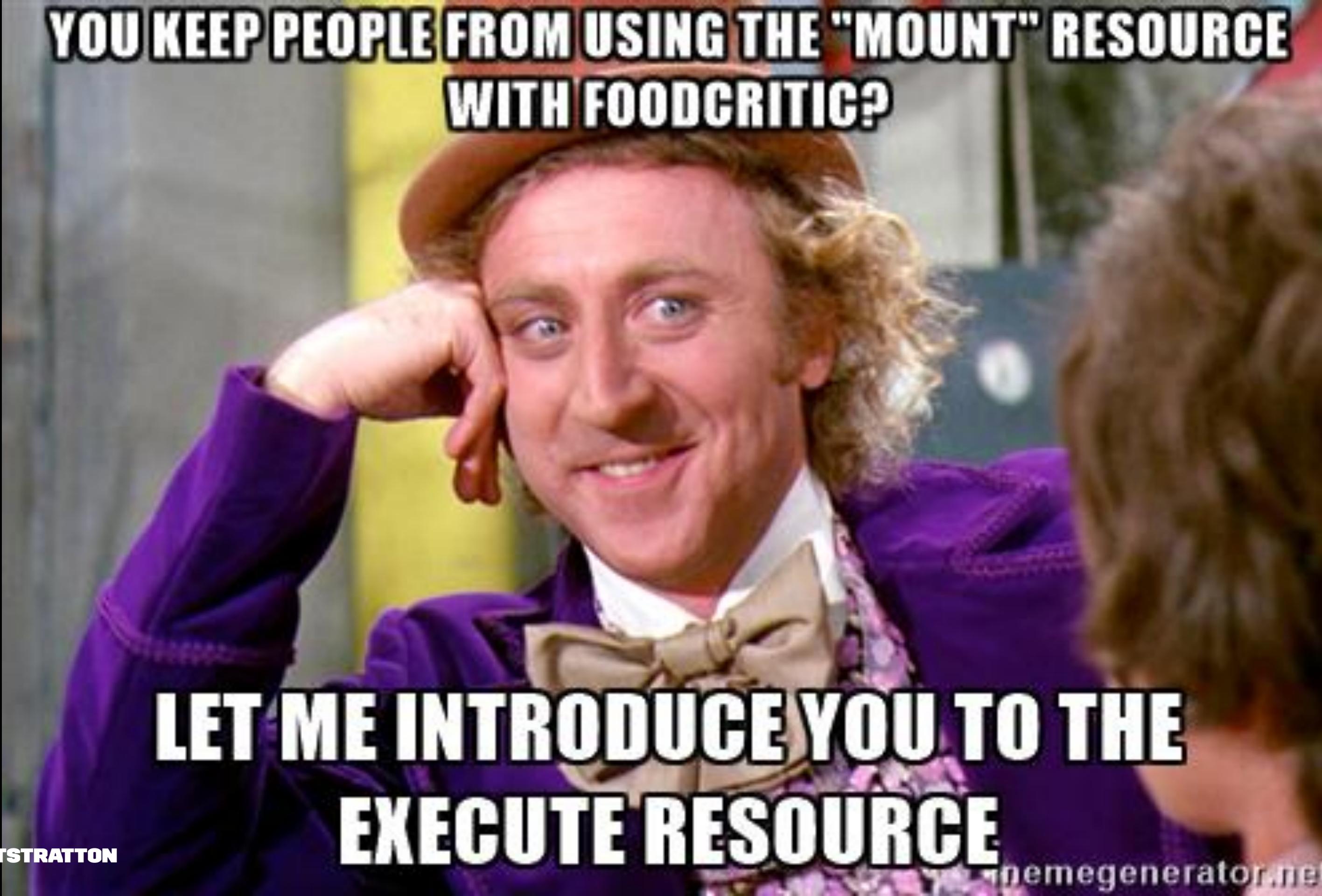






- » If you spend time keeping people from doing x, y, or z
- » They will instead do a, b, or c to get the outcome they want

**YOU KEEP PEOPLE FROM USING THE "MOUNT" RESOURCE
WITH FOODCRITIC?**



**LET ME INTRODUCE YOU TO THE
EXECUTE RESOURCE**

PROBLEM WITH DISTRIBUTED CONFIGURATION MANAGEMENT

- » Developer reads on Stack Overflow that disabling selinux will make his Node app work better.
- » Developer updates his cookbook to disable selinux
- » Sysadmins get fired because of 3vil haxx0rz

THE BETTER WAY

- » Developer reads on Stack Overflow that disabling selinux will make his Node app work better.
- » Developer updates his cookbook to disable selinux
- » Developer runs local tests which include compliance checks
- » Compliance checks test for state of selinux
- » Tests fail. Developer says "Welp, I guess I can't do that."



TRUST BUT VERIFY

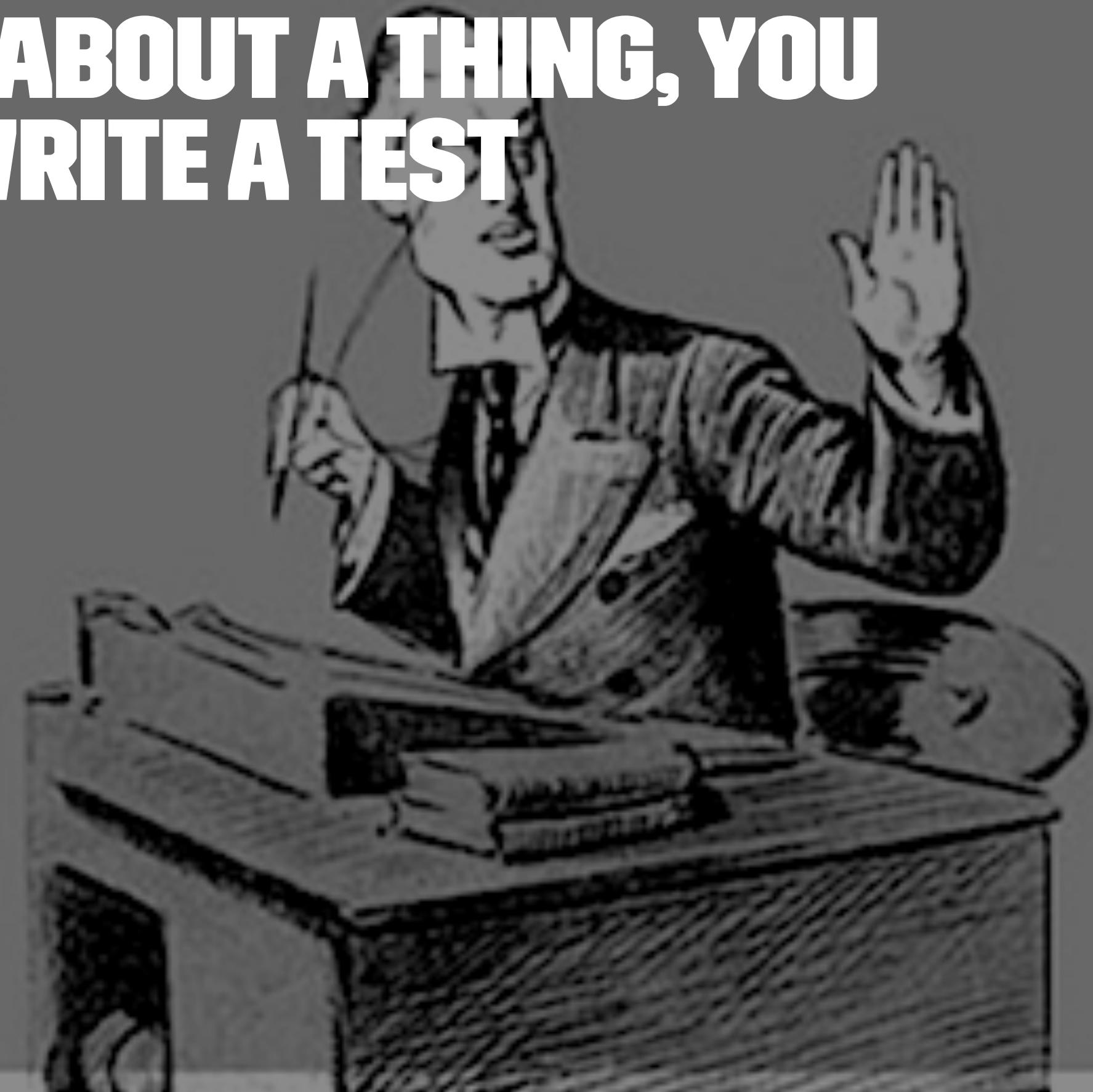
WHAT IF THE DEVELOPERS DON'T RUN THOSE LOCAL TESTS?

The pipeline catches them.

They'll do better next time.

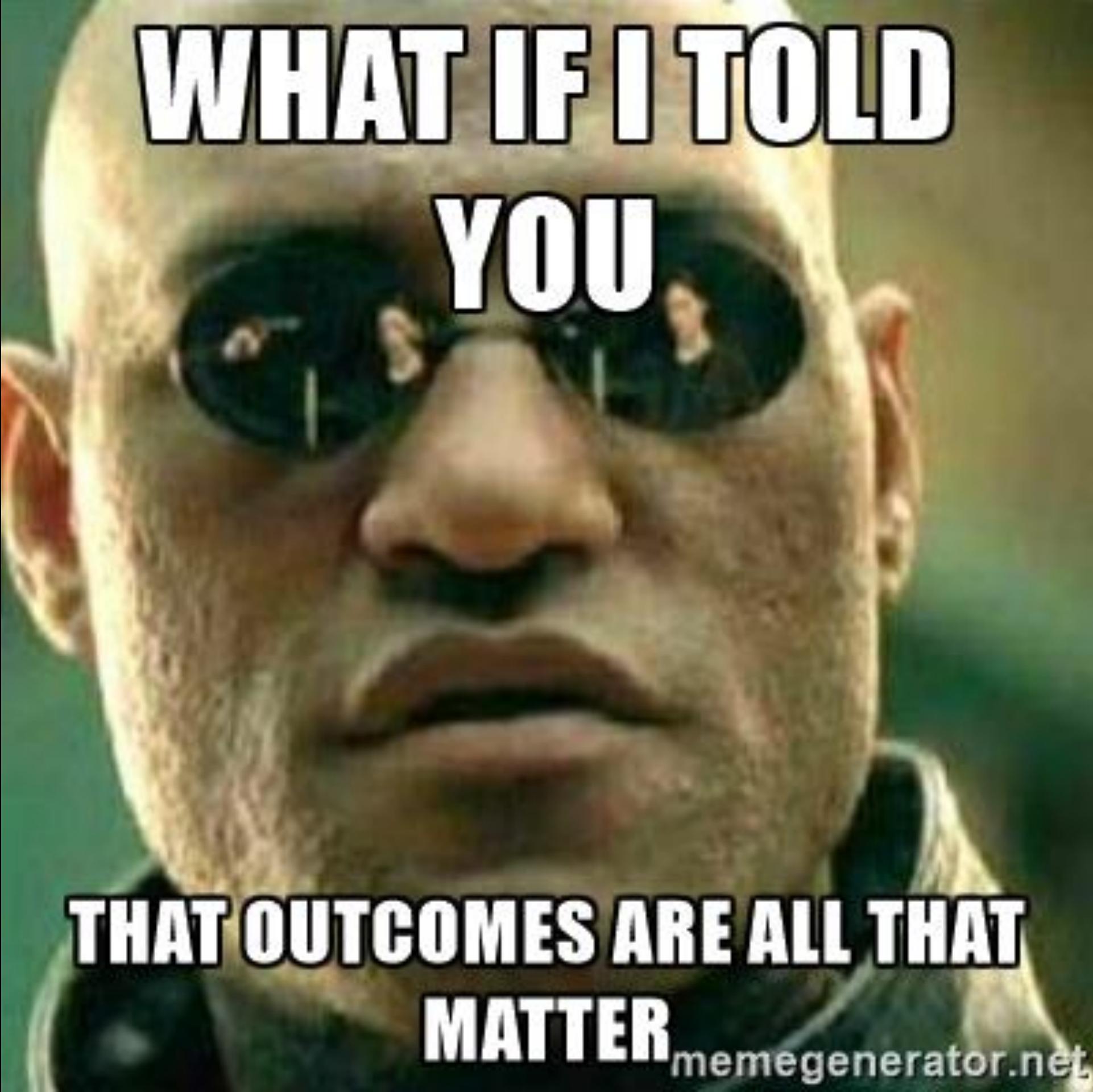
**IF YOU TRULY CARE ABOUT A THING, YOU
CARE ENOUGH TO WRITE A TEST**

I'm too busy to
tell people how
busy I am.



som~~e~~e cards

@MATTSTRATTON



**WHAT IF I TOLD
YOU**

**THAT OUTCOMES ARE ALL THAT
MATTER**

PLEASE DEMOCRATIZE



YOUR COMPLIANCE TESTING

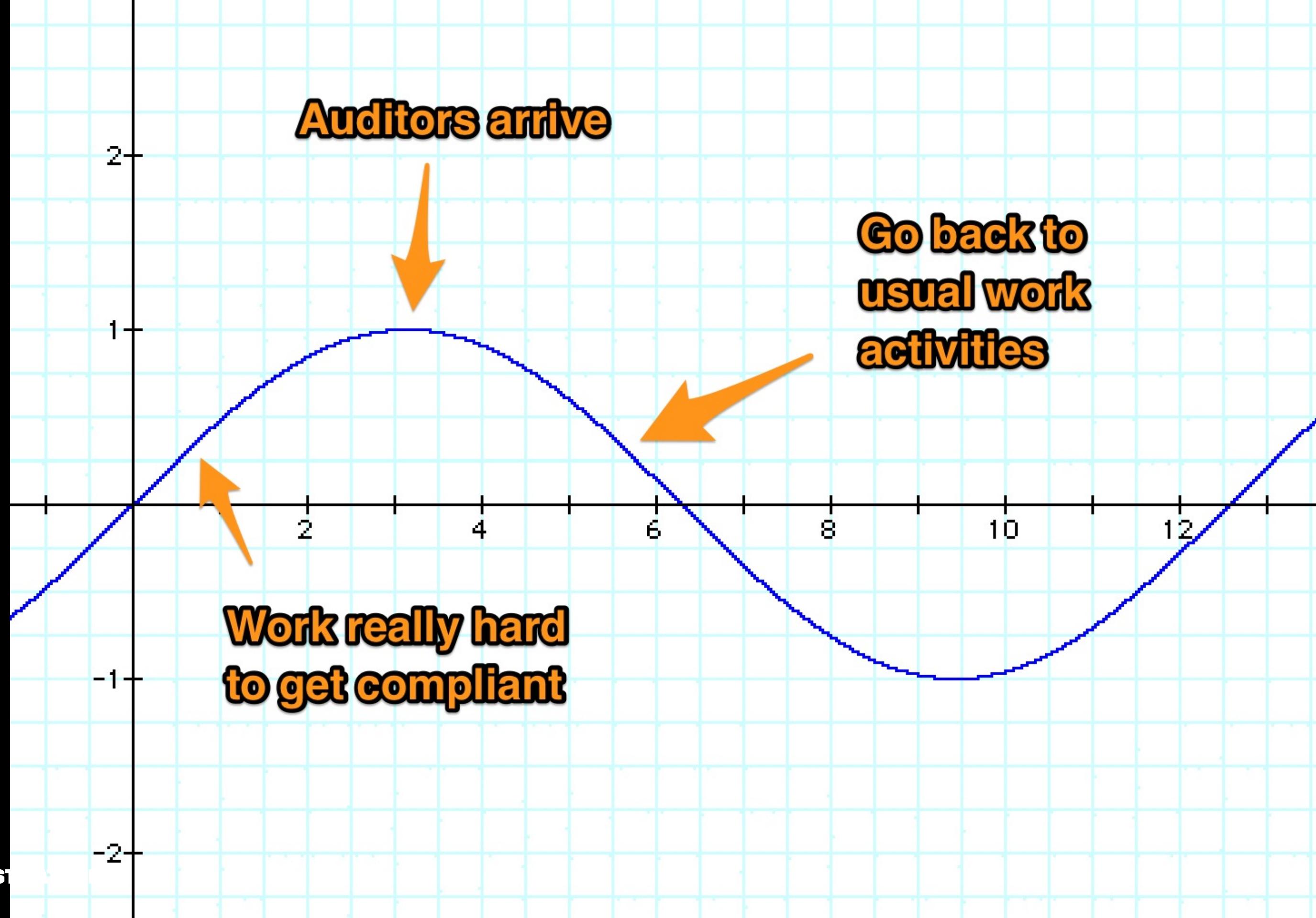


**THE VENDOR IS NOT
THE ISSUE HERE, DUDE**

```
> grep '^Protocol' /etc/ssh/sshd_config | sed 's/Protocol //'  
2
```

VS

```
control 'ssh-1234' do  
  impact 1.0  
  title 'Server: Set protocol version to SSHv2'  
  desc "  
    Set the SSH protocol version to 2. Don't use legacy  
    insecure SSHv1 connections anymore...  
"  
  
  describe sshd_config do  
    its('Protocol') { should eq 2 }  
  end  
end
```



TO REVIEW

- » Treat your pipeline as code
- » Trust (but verify) your domain experts
- » Focus on the what, not the how. Outcomes, outcomes, outcomes.
- » Use your production audit tests in your pipeline
- » Did I mention test?

QUESTIONS?



RESOURCES

- » Sidney Dekker - Field Guide to Human Error
- » github.com/mattstratton/speaking
- » twitter.com/mattstratton
- » speakerdeck.com/mattstratton
- » arresteddevops.com