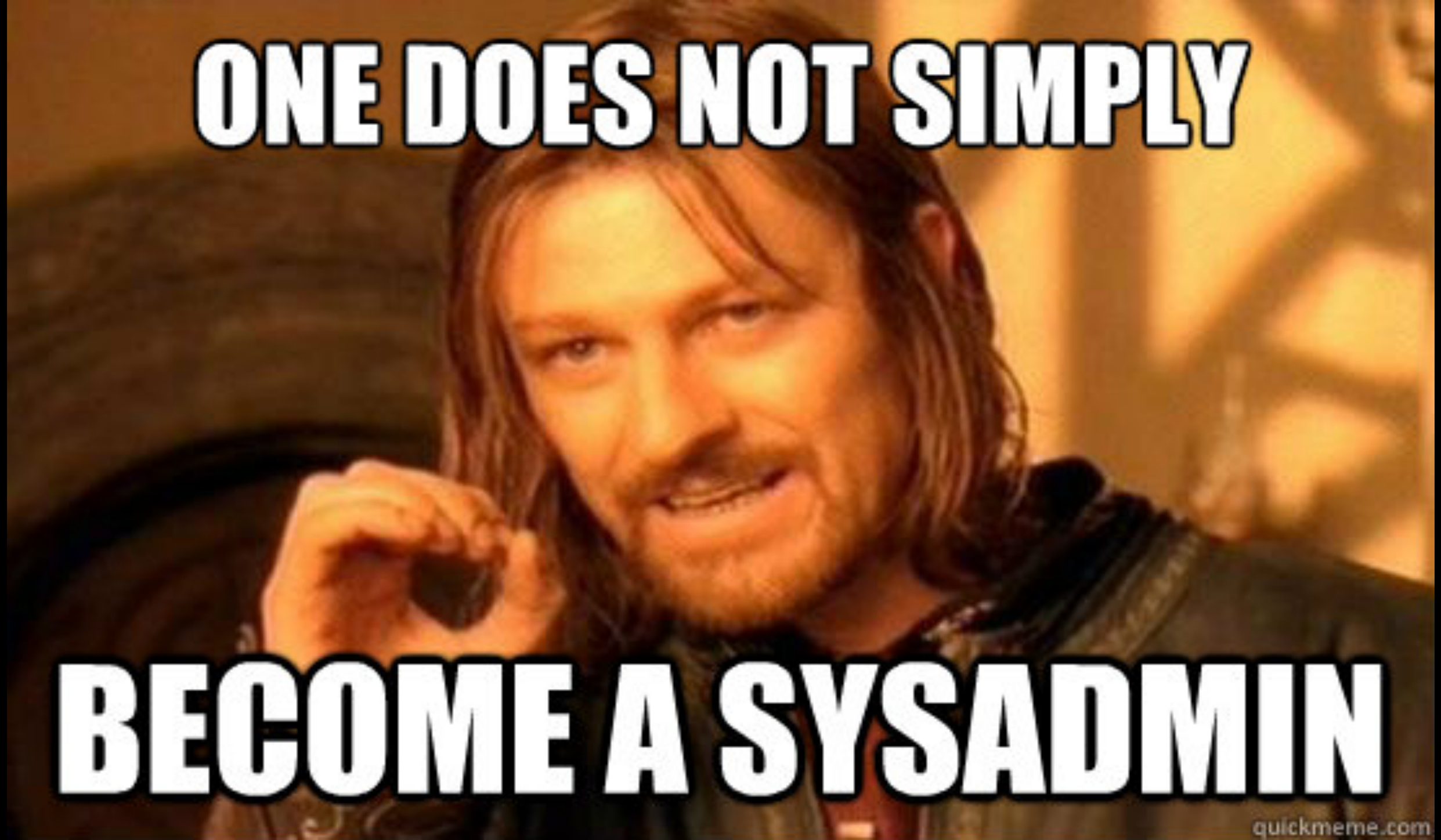
SHIFTING LEFT SECURELY

@MATTSTRATTON

WHOAMI

@mattstratton

@MATTSTRATTON


ONE DOES NOT SIMPLY
BECOME A SYSADMIN
quickmeme.com

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

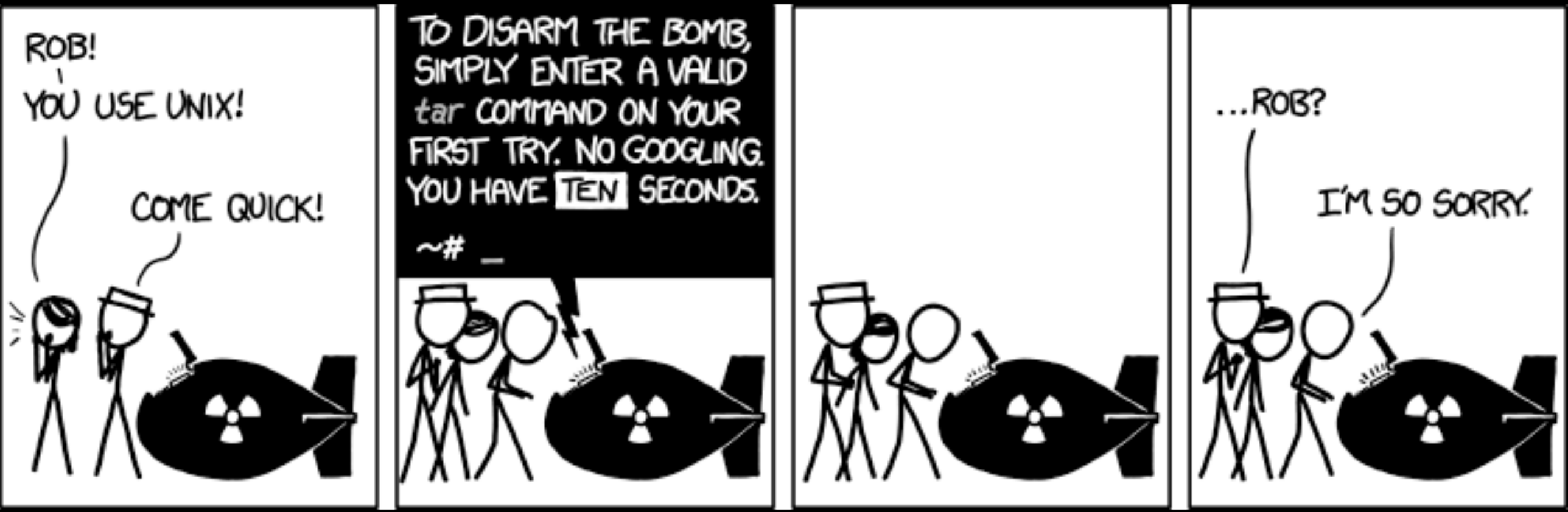
13 Server Administration · 28 Microsoft SQL Server · 31 IT Operations

14 IT Service Management · 19 Powershell · 24 Virtualization · 9 Automation

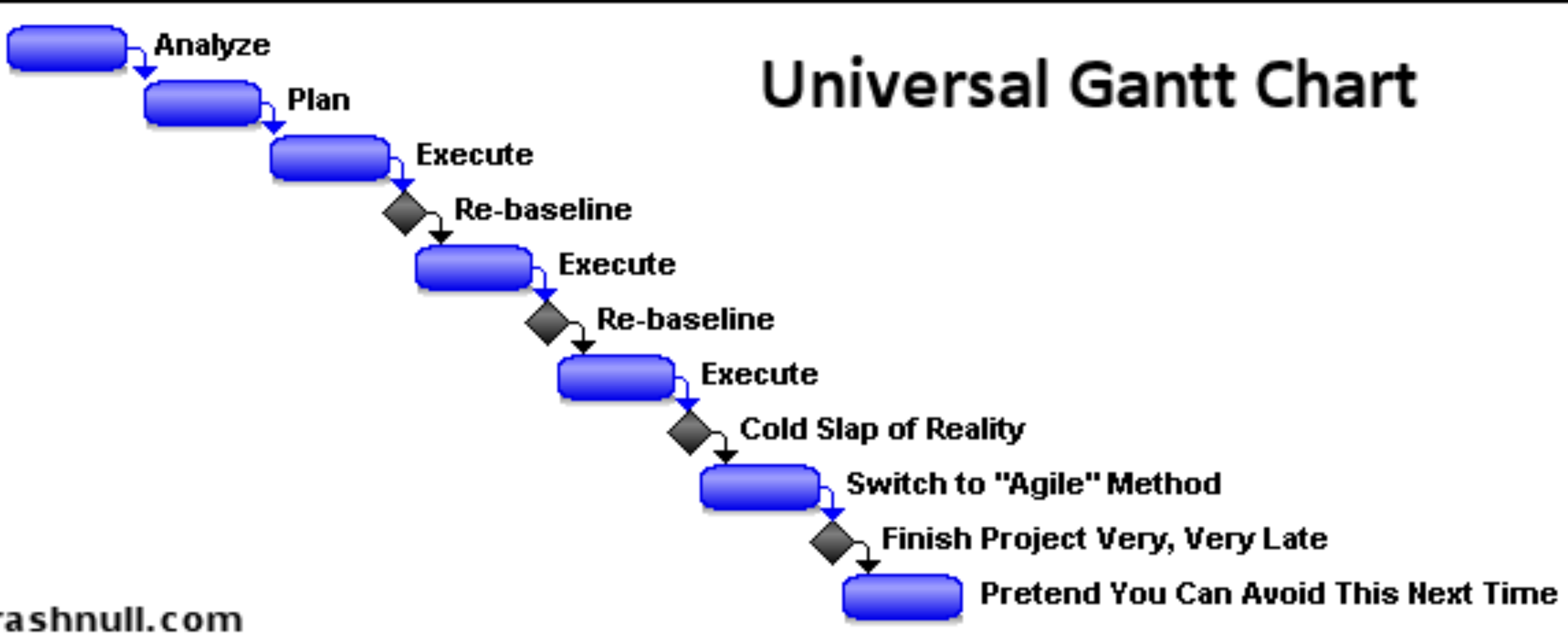
9 Microsoft Technologies · 18 Data Center · 5 Release Management

@MATTSTRATTON

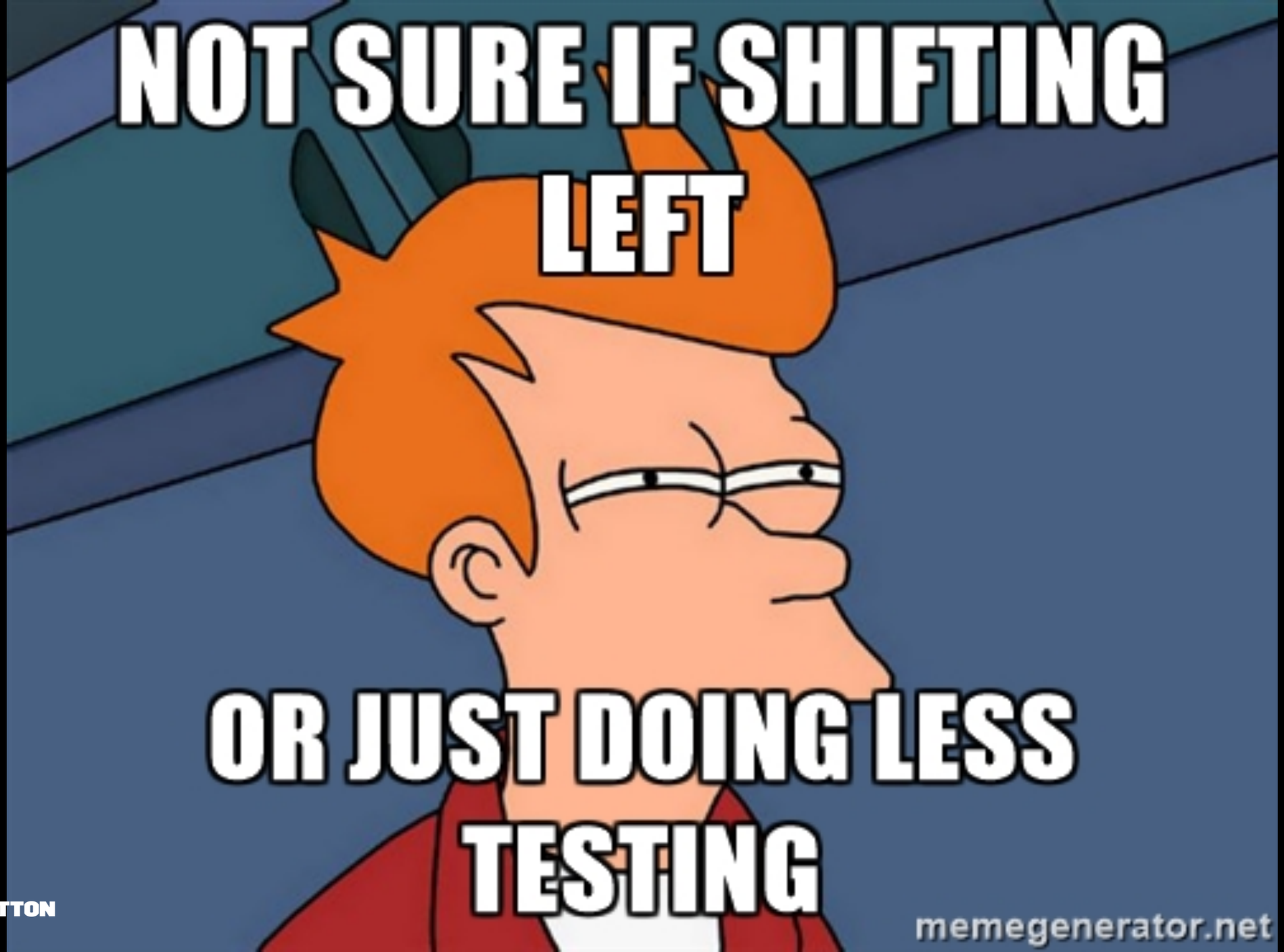

- I'VE MADE A HUGE MISTAKE.
@MATTSTRATTON



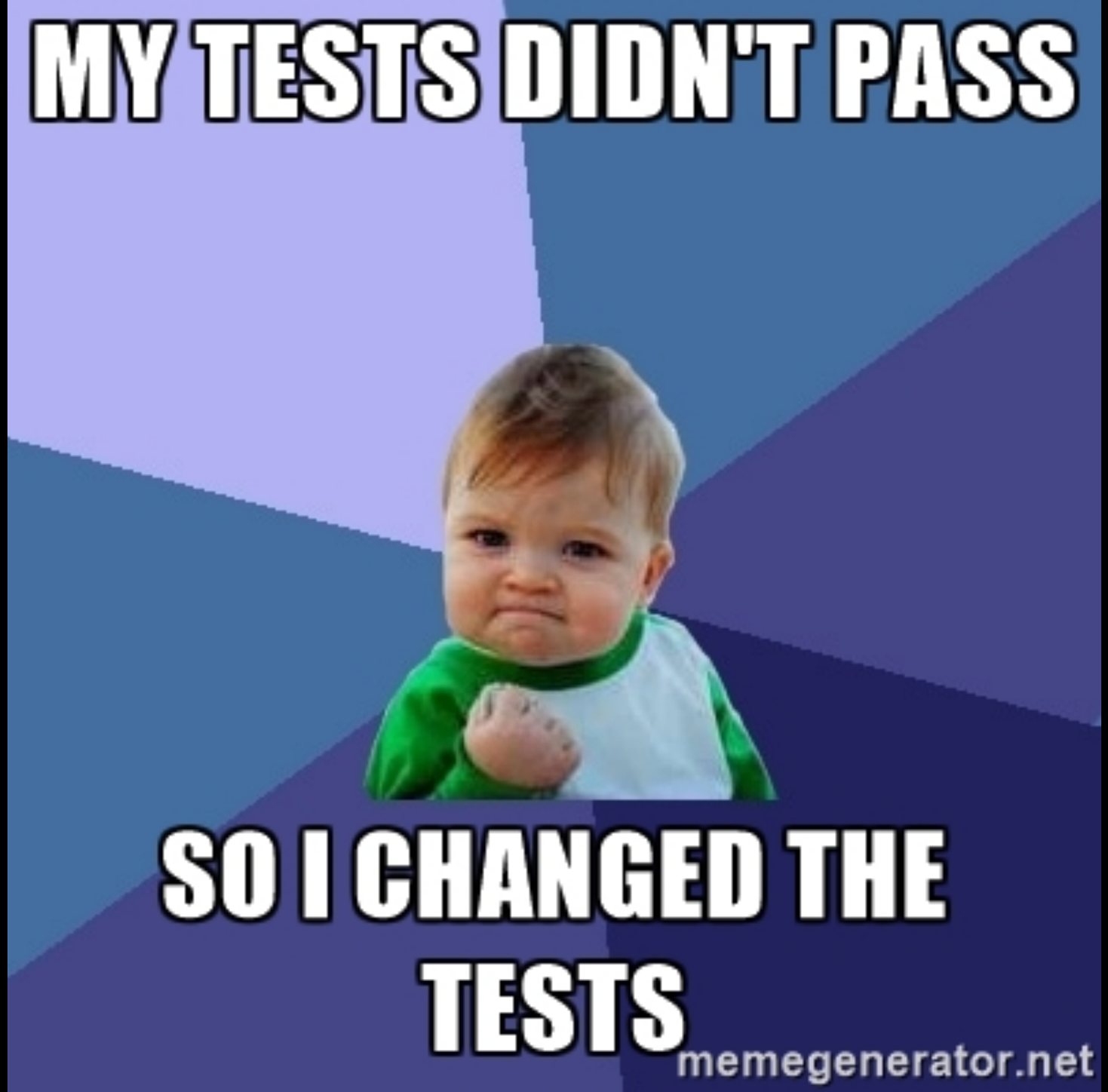
@MATTSTRATTON


Universal Gantt Chart
Analyze
Plan
Execute
Re-baseline
Execute
Re-baseline
Execute
Cold Slap of Reality
Switch to "Agile" Method
Finish Project Very, Very Late
Pretend You Can Avoid This Next Time
rashnull.com

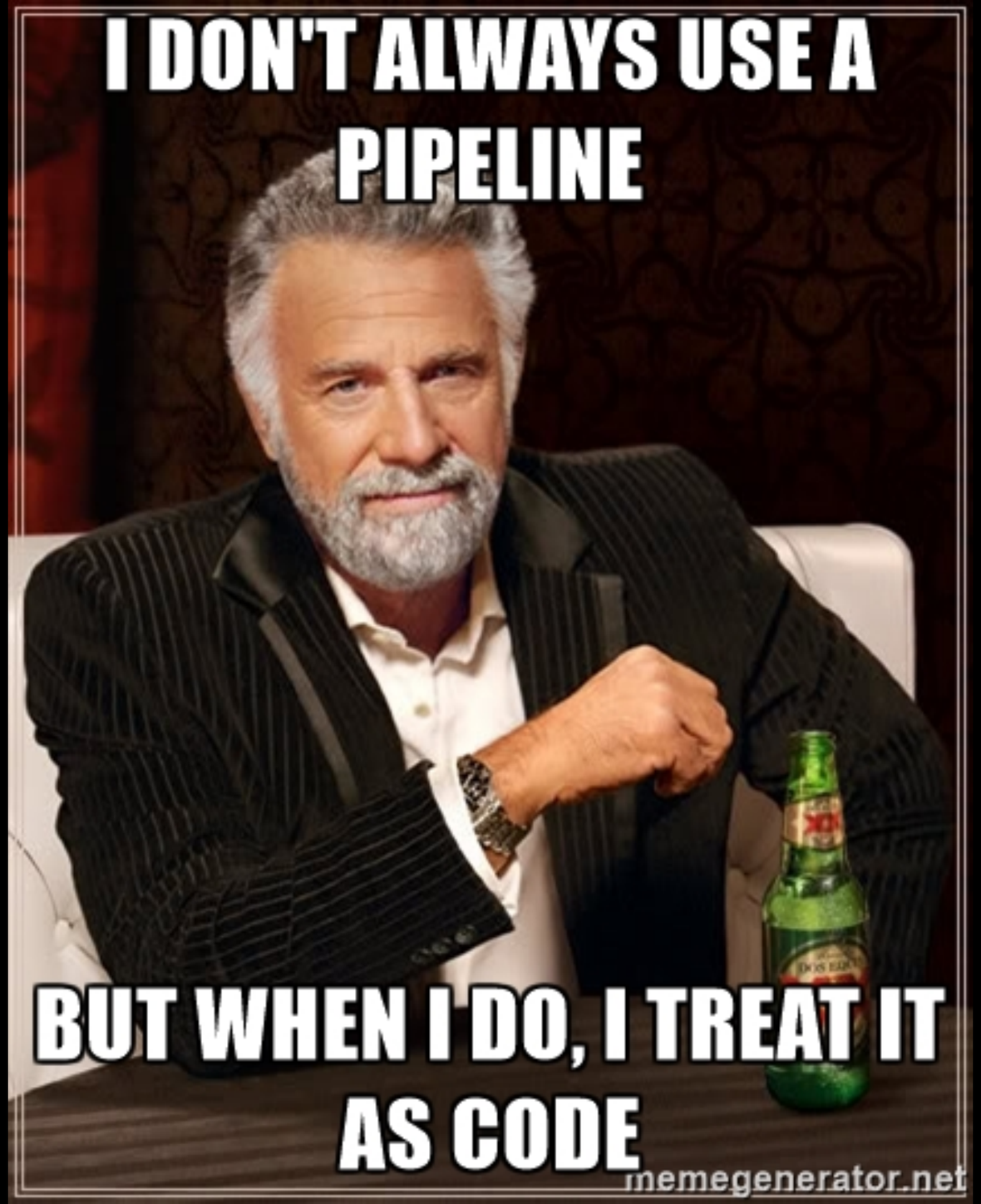

EPICFAIL.com



@MATTSTRATTON



@MATTSTRATTON

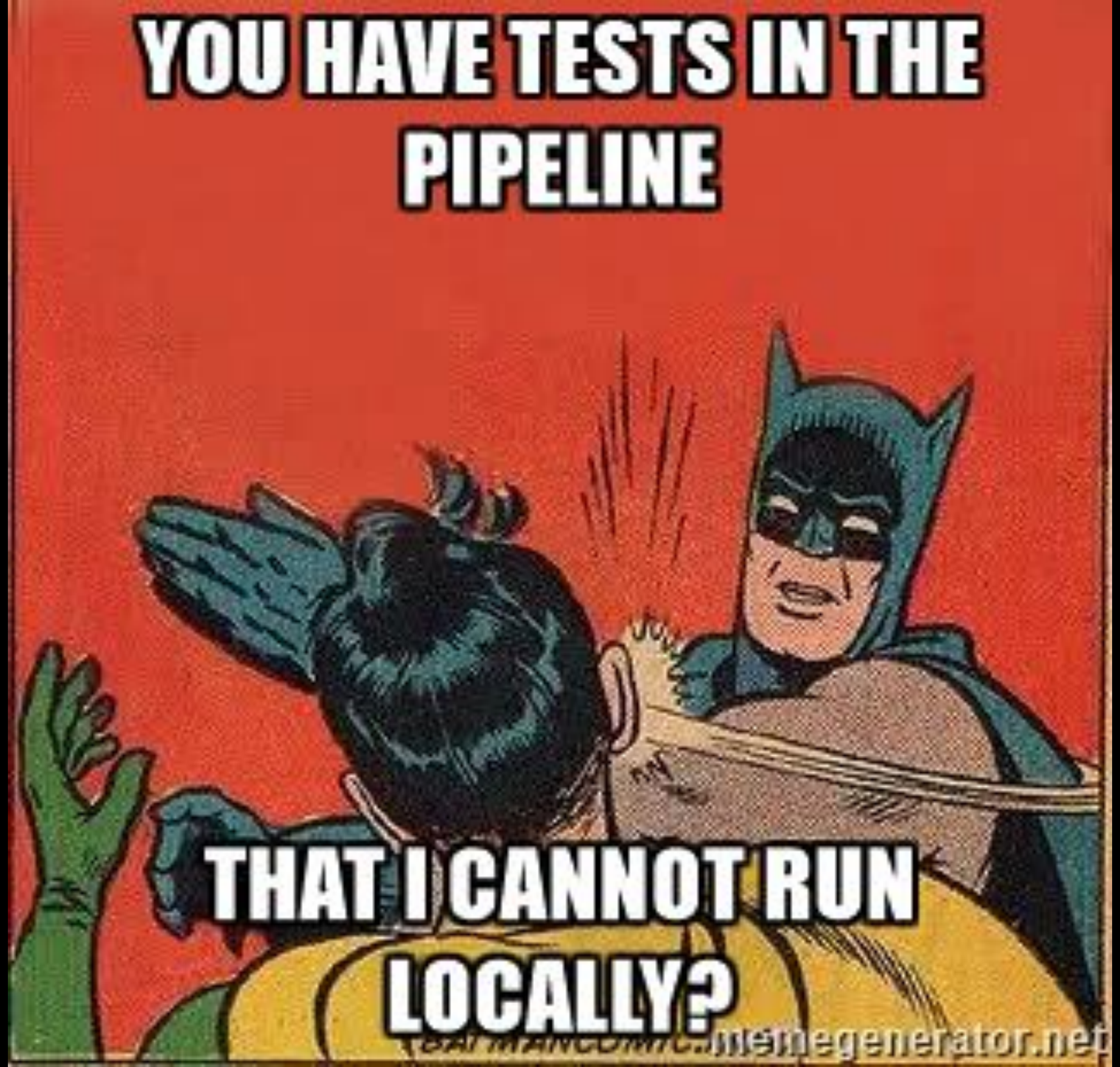


@MATTSTRATTON

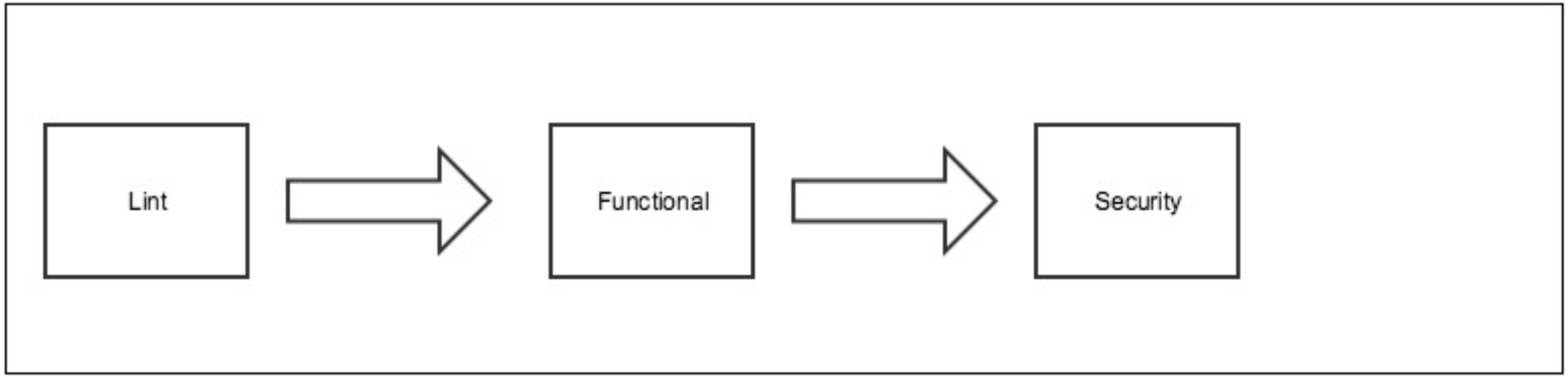
HOW DOES THIS HELP ME WITH SECURITY?

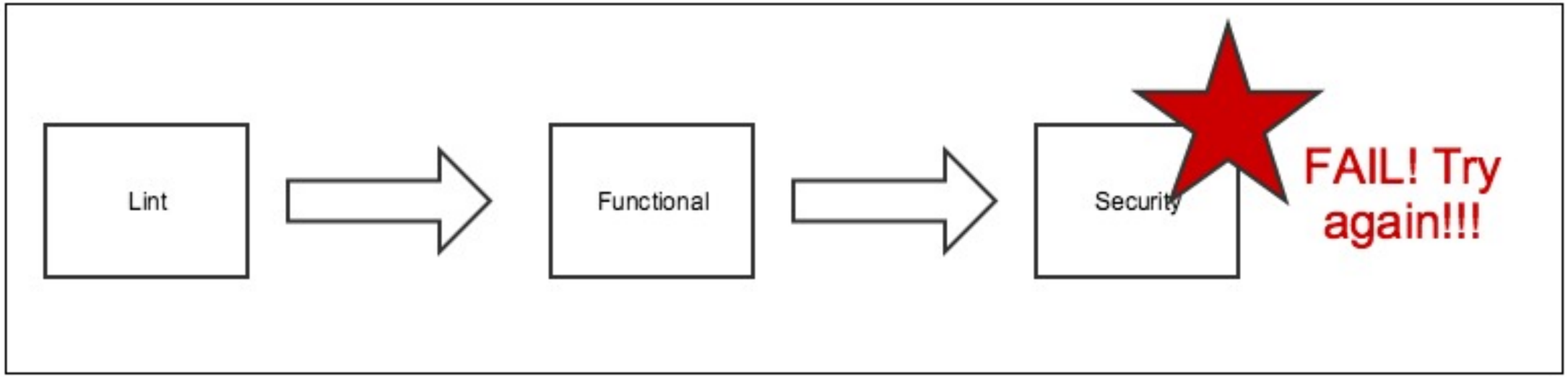
WHAT IF WE CONTINUOUSLY TESTED FOR SECURITY

INSTEAD OF WAITING FOR A "HARDENING SPRINT"?

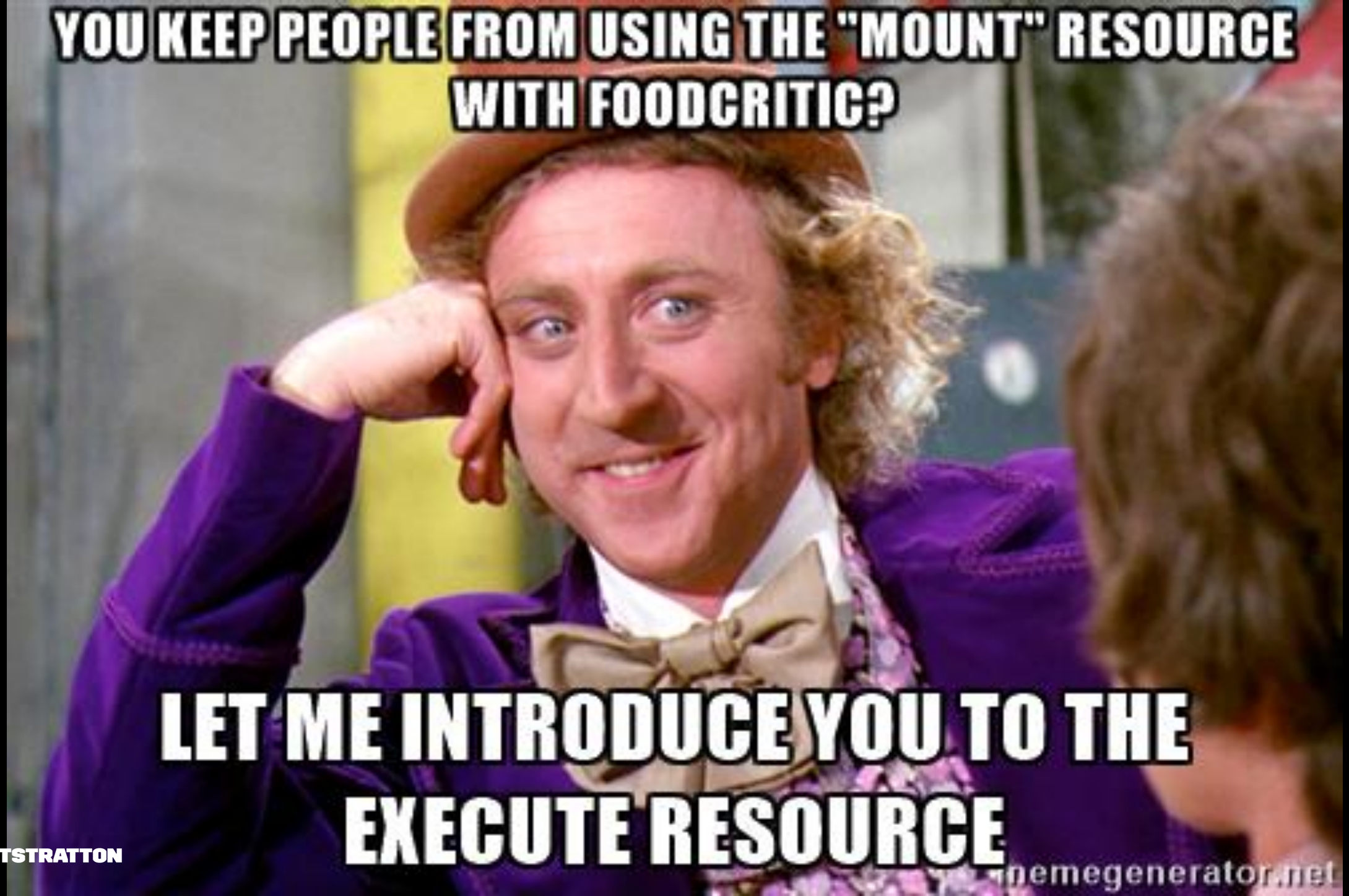


@MATTSTRATTON


Lint
Functional
Security


Lint
Functional
Security
FAIL! Try again!!!

- 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



@MATTSTRATTON

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

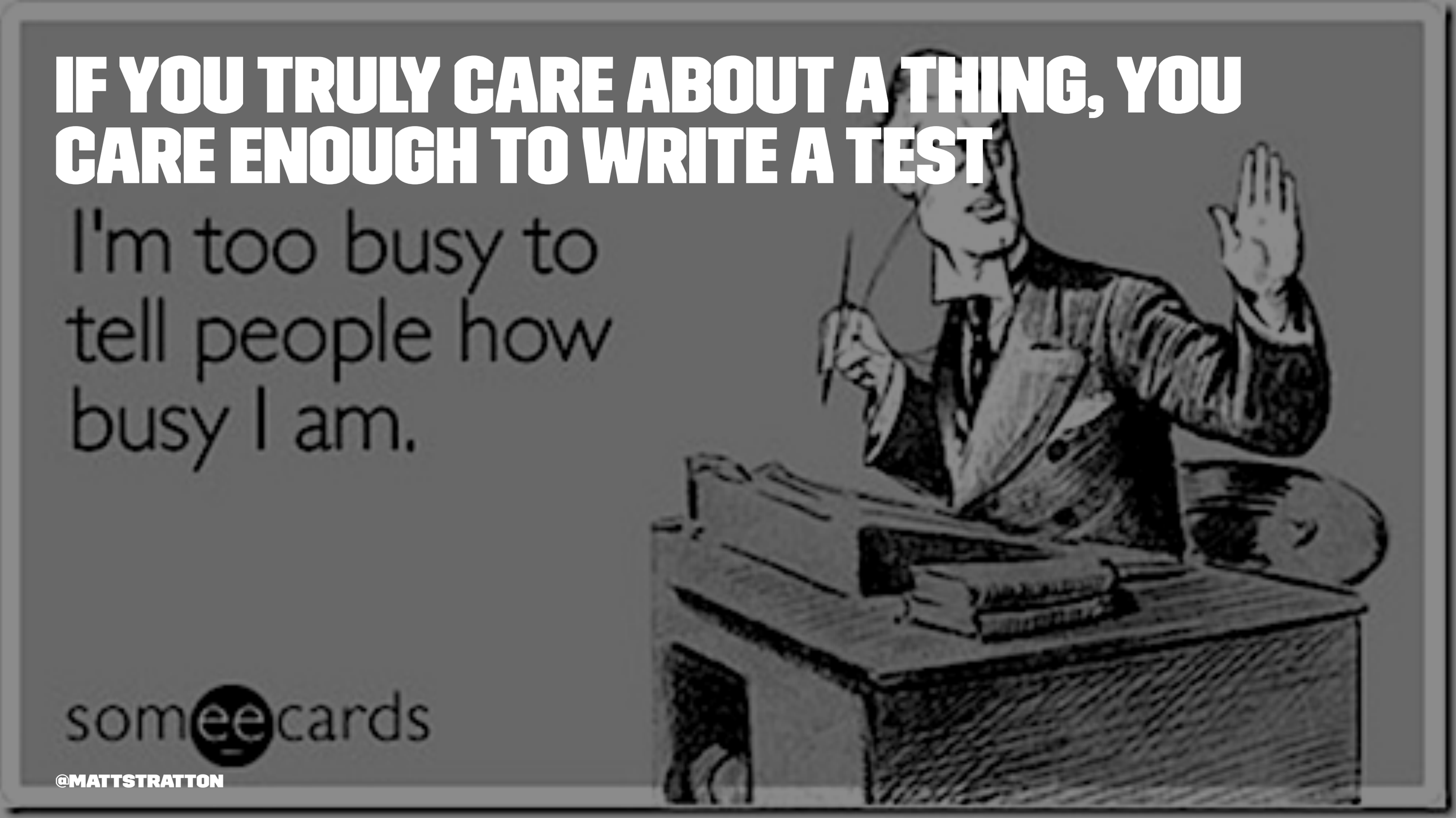
» Tests fail. Developer says "Welp, I guess I can't do that."

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

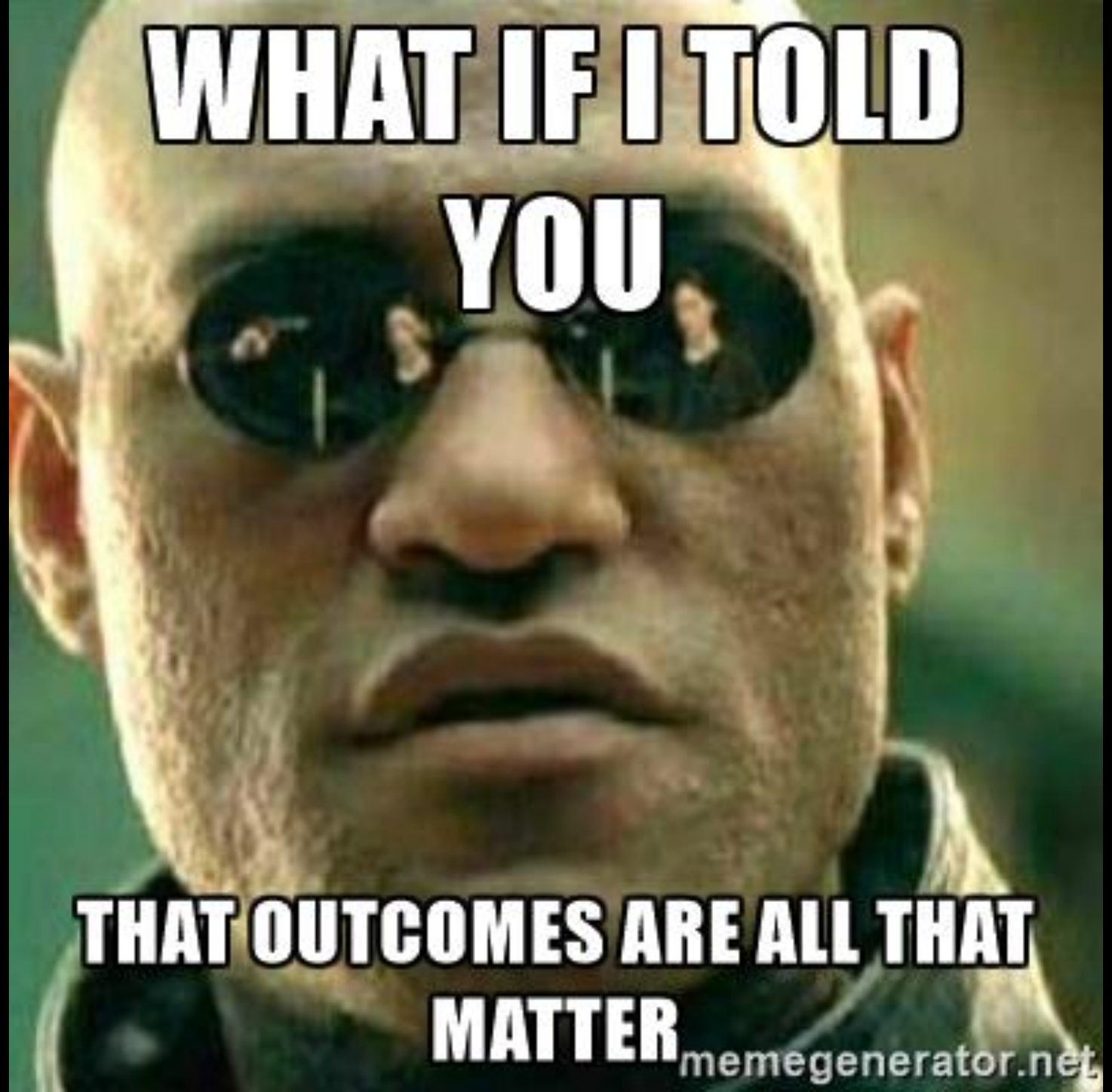
The pipeline catches them.

They'll do better next time.

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



@MATTSTRATTON



@MATTSTRATTON

@MATTSTRATTON

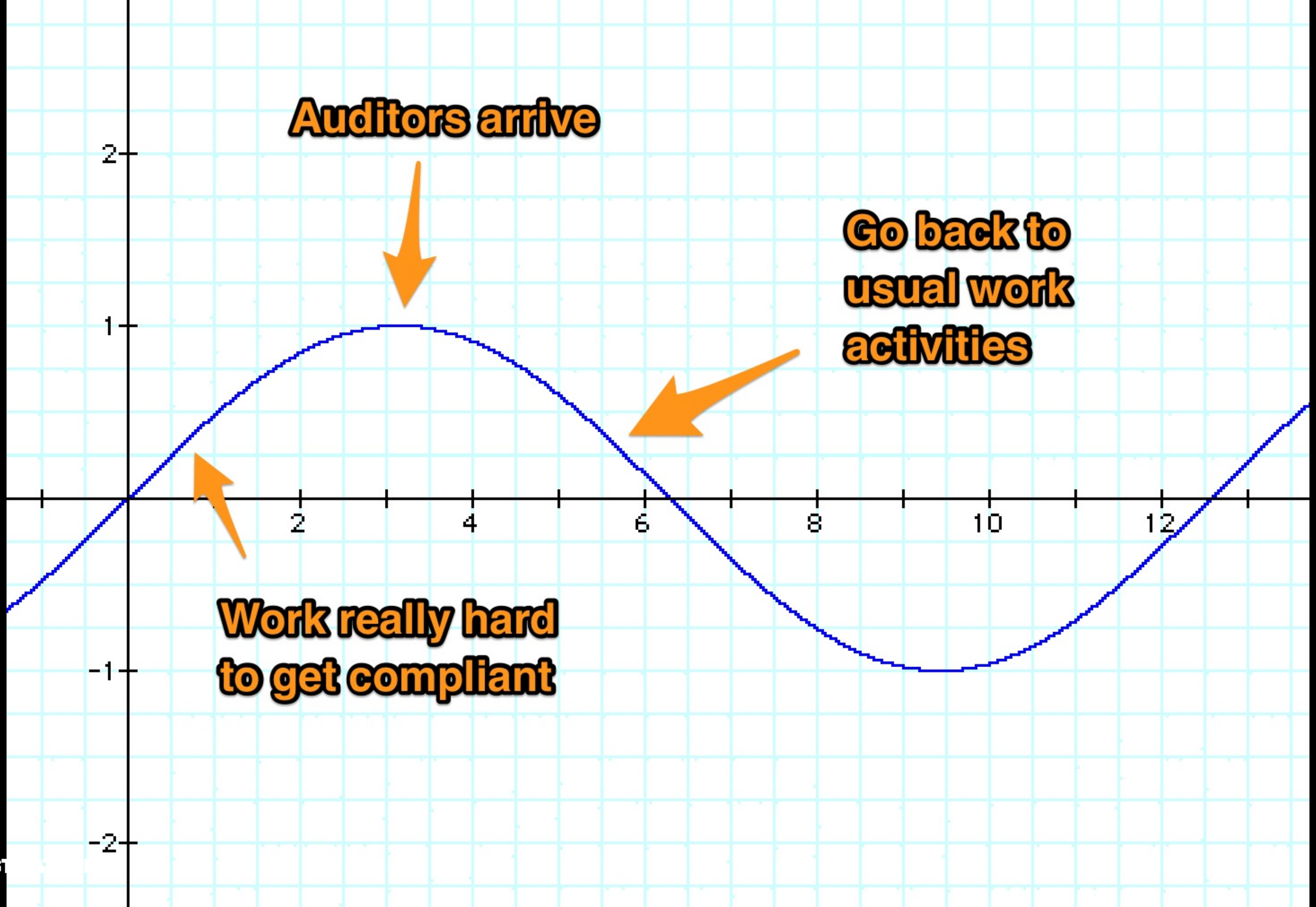
@MATTSTRATTON

```
> 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
```


Auditors arrive
Go back to usual work activities
Work really hard to get compliant
2
1
-1
-2
2
4
6
8
10
12

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?

@MATTSTRATTON

RESOURCES

» Sidney Dekker - Field Guide to Human Error

» github.com/mattstratton/speaking

» twitter.com/mattstratton

» speakerdeck.com/mattstratton

» arresteddevops.com