Defense at Scale

an optimistic #infosec talk in two slides

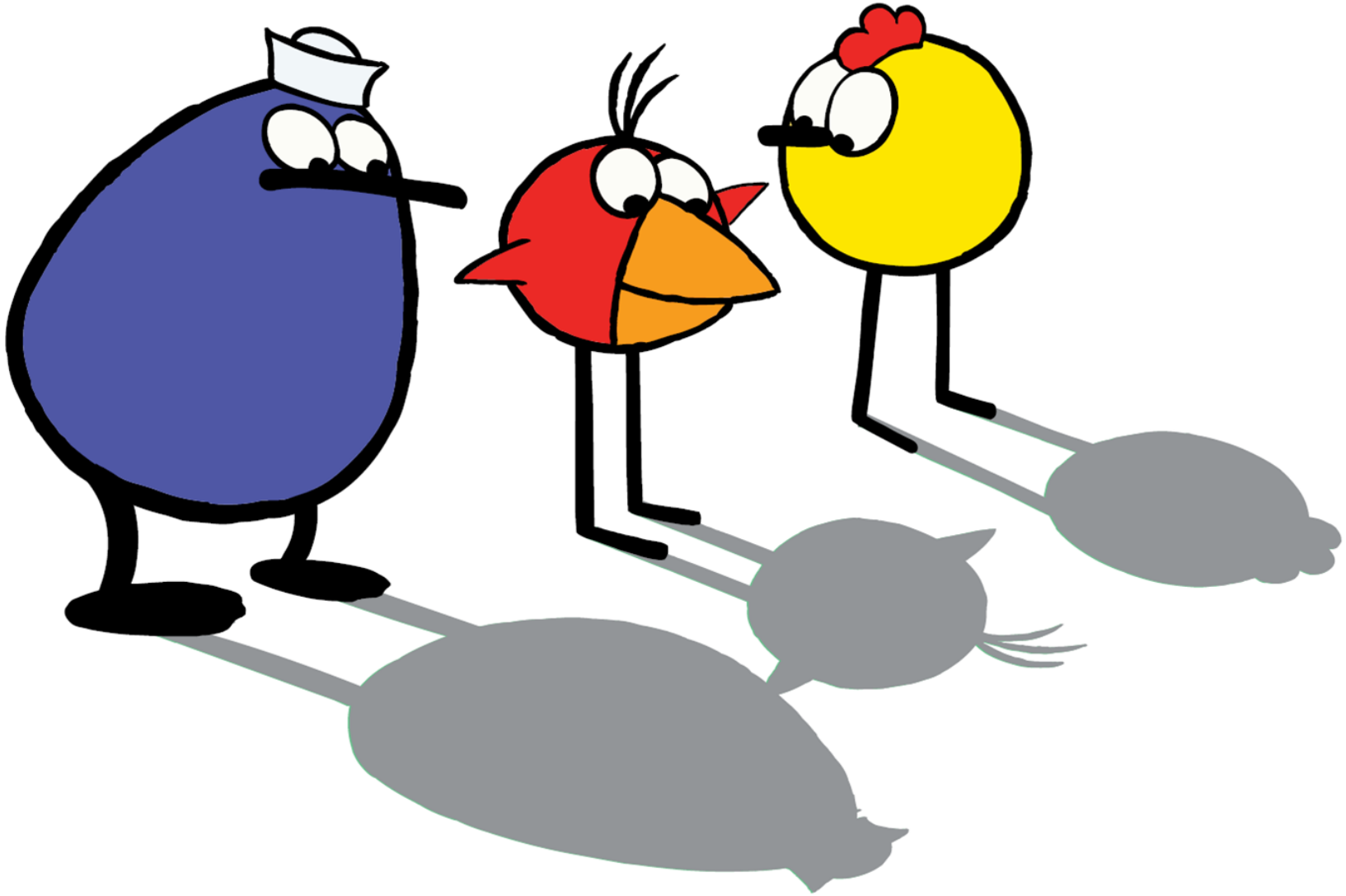
BSidesNYC

2016

https://v.gd/defenseAtScale

Jan Schaumann

@jschauma



@jschauma

https://v.gd/defenseAtScale03

Defense at Scale

an optimistic #infosec talk in two or more slides

BSidesNYC

2016

Jan Schaumann

@jschauma

Justin Schuh
@justinschuh

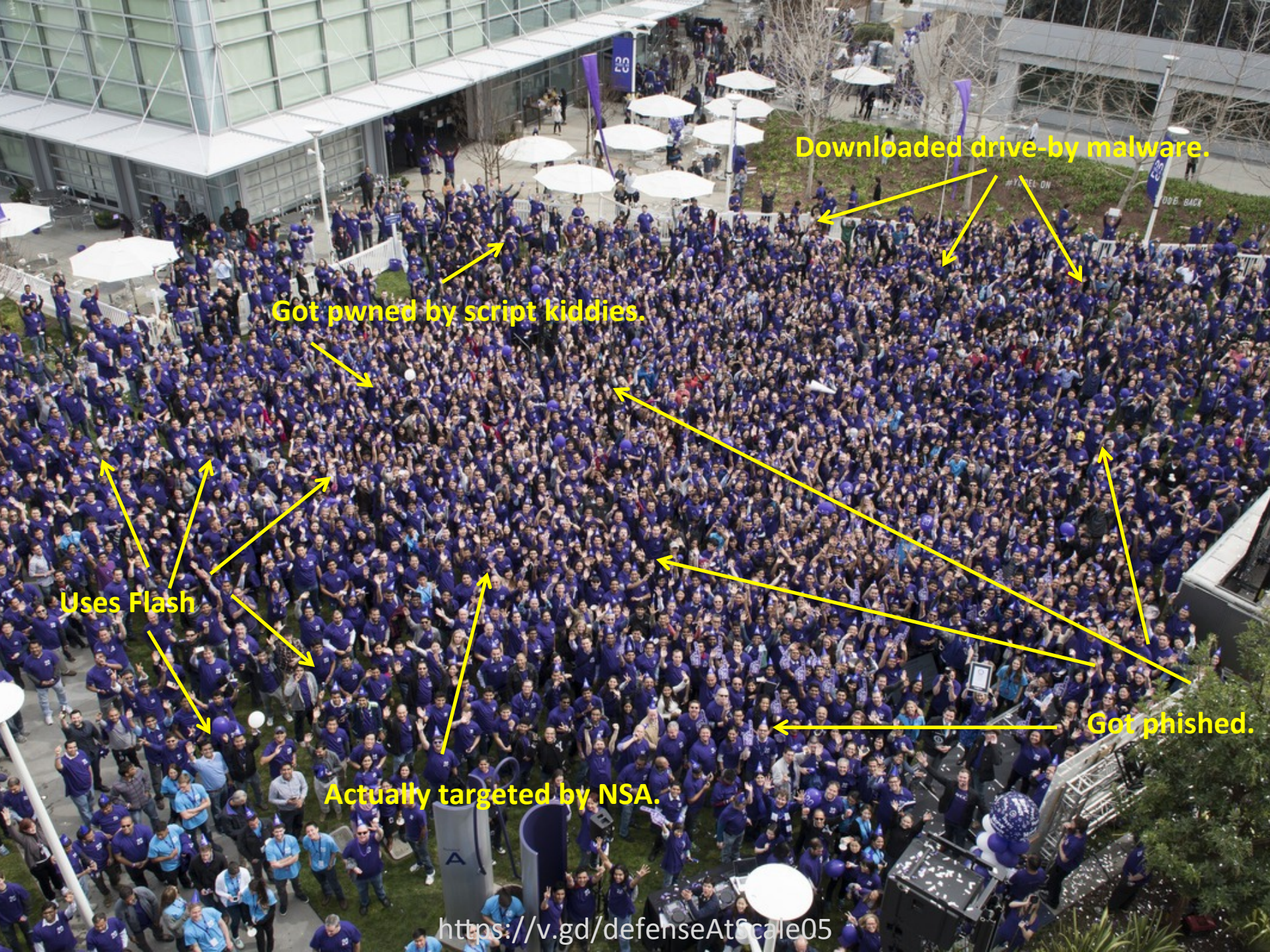
Follow

Security at its core is about reducing attack surface. You cover 90% of the job just by focussing on that. The other 10% is mostly luck.

RETWEETS 102 LIKES 102

4:51 PM - 8 Jan 2016

https://v.gd/defenseAtScale04



https://v.gd/defenseAtScale05

https://v.gd/defenseAtScale06

Jan Schaumann
@jschauma

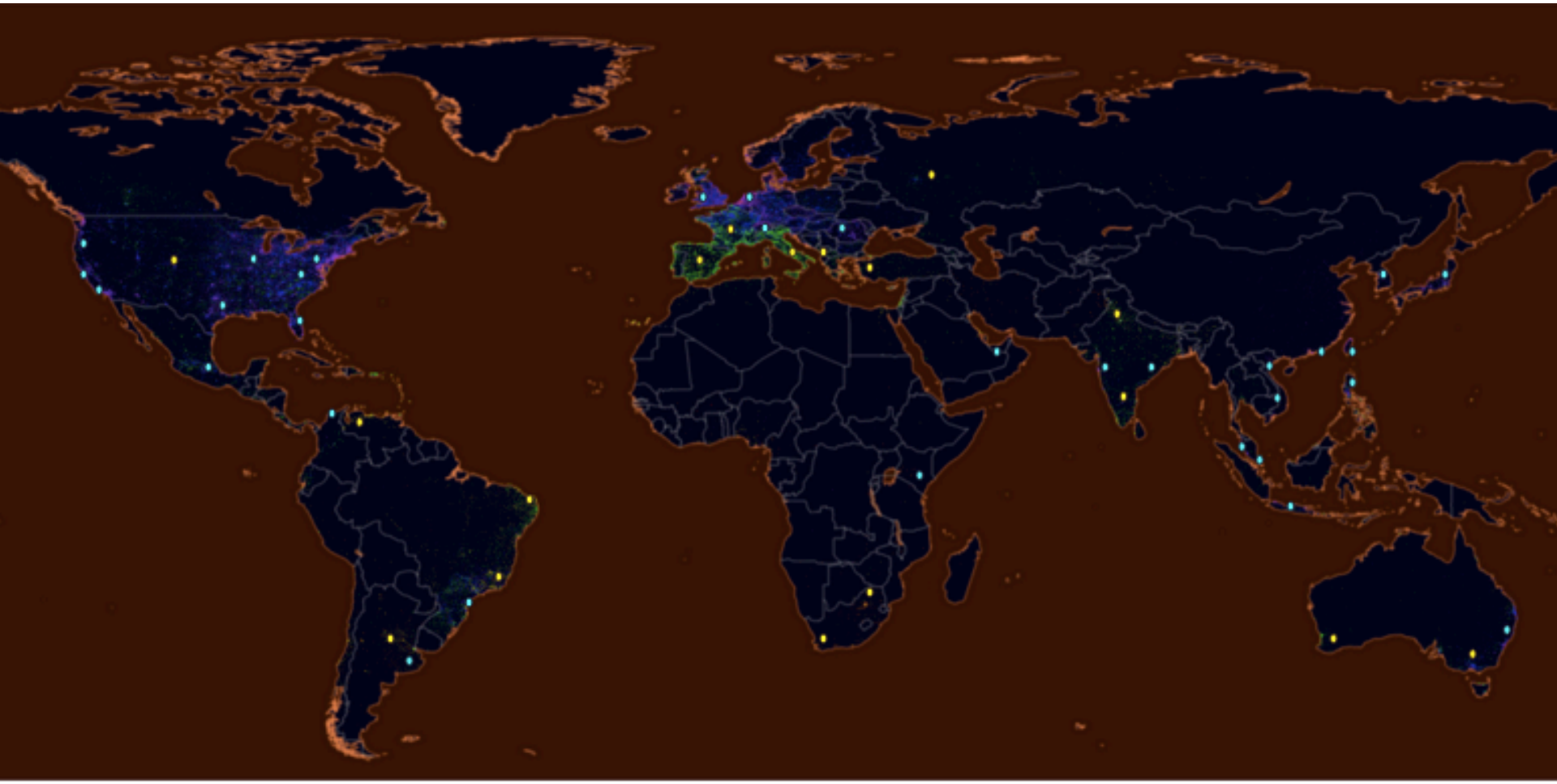
Follow

$ uptime
 2:26PM up 3429 days, 11:59, 1 user, load averages: 0.33, 0.27, 0.29
$ uname -rs
FreeBSD 4.11

RETWEETS 93 LIKES 130

2:29 PM - 5 Jan 2016

https://v.gd/defenseAtScale07




ORACLE
Seagate
SAMSUNG
Ruby
open source
JavaScript
SQL Server 2008
Logitech
Google
OpenOffice.org
YAHOO!
CSS
W3C
Windows
jQuery
redhat
FFMPEG
IBM
AJAX
NVIDIA
Sun
microsystems
php
YouTube
MySQL
MediaWiki
GNOME
Java
GNU
rpm
SONY
<?xml?>
Apache
ebay
verizon
Adobe
intel
FreeBSD
OpenBSD
NetBSD
DragonFly BSD
Darwin

You get to drink from the FIREHOSE!!!

No caption necessary.


UNDER STAFFED!
UNDER STAFFED EVERY WHERE!
memegenerator.net


VERIFIED POC
DEV PROBLEM NOW
memegenerator.net

Skin in the Game

- Who carries the cost of fixing security problems?
- Who pays out the Bug Bounty for the same set of command-injection or XSS vulnerabilities?
- Who is incentivized to improve security?

Prioritize.

100% secure is impossible –
but that's ok.

Raising the cost of an attack is often sufficient. (Know your Threat Model.)

Fucks don’t scale.

“Prevent, Detect, React”

“Prevent, Detect, React”

Firewalls, Monitoring, Patching

“Prevent, Detect, React”

Firewalls, Monitoring, Patching

Vendor Crap, Vendor Crap, ¯_(ツ)_/¯

"Are vulnerabilities in software dense or sparse? If they are sparse, then every one you find and fix meaningfully lowers the number of avenues of attack that are extant. If they are dense, then finding and fixing one more is essentially irrelevant to security and a waste of the resources spent finding it. Six-take-away-one is a 15% improvement. Six-thousand-take- away-one has no detectable value." *Geer/Schneier*

https://v.gd/defenseAtScale08


Admirals Clu
Enter here for expedited screening.
Attention
Your safety is our priority

If you can make things better without making things worse, do it.

Even if it doesn't make things perfect.

https://v.gd/defenseAtScale09

If what you're doing doesn't make things better, stop doing it.

Even if you've always done it.

Even if it took a lot of effort to start doing.

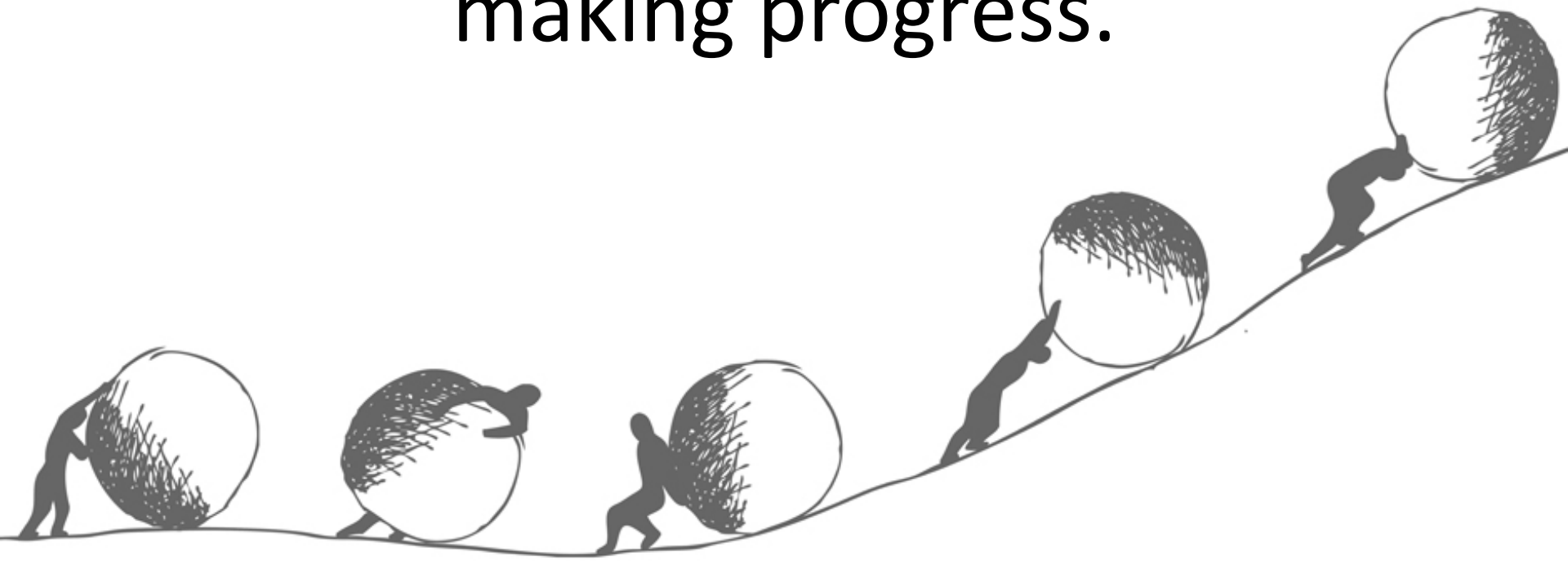
https://v.gd/defenseAtScale09

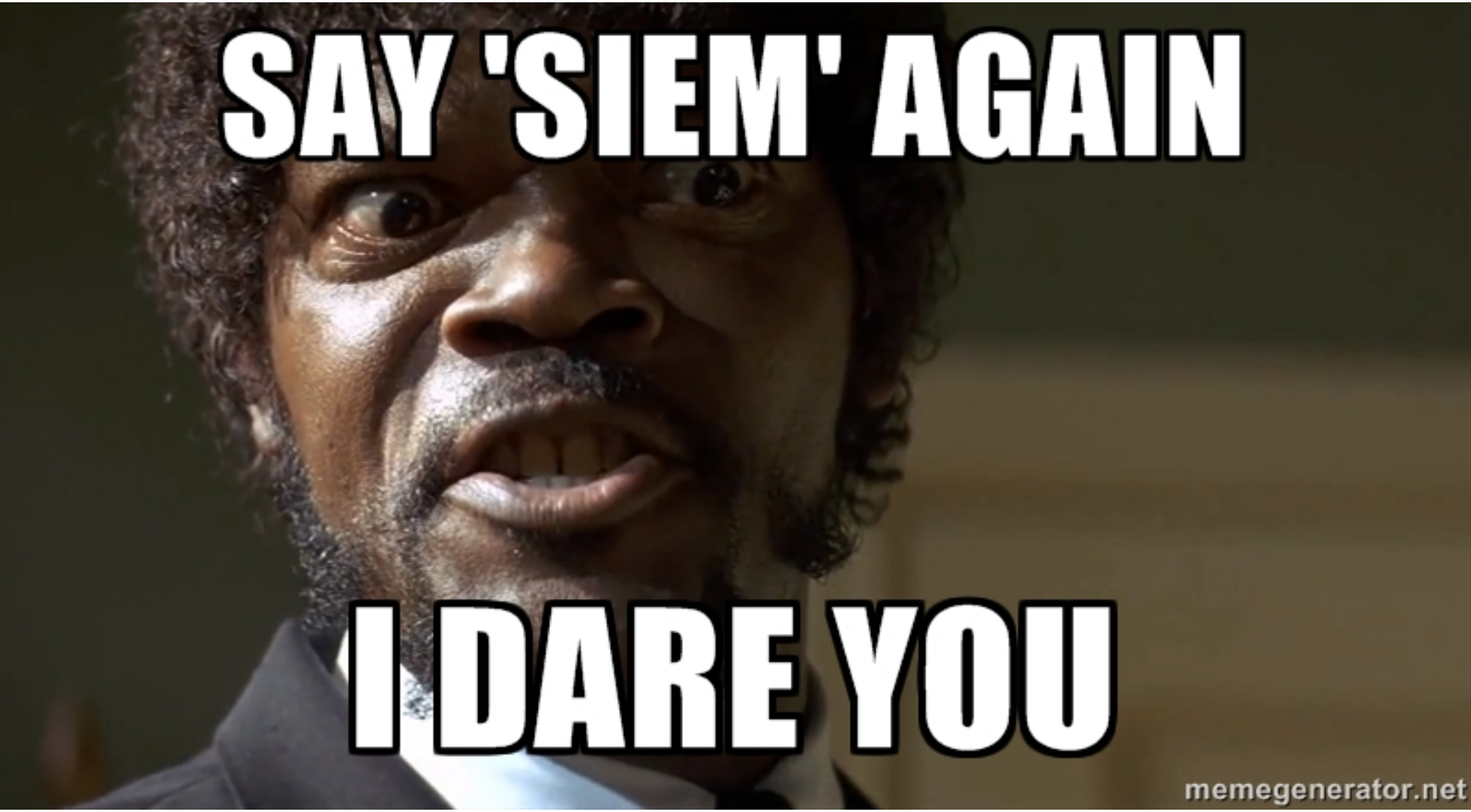
Think big.

Vulnerabilities are not sparse.

Don’t fix individual bugs, focus on eliminating entire *vulnerability classes* instead.

If you keep fixing the same issue over and over again, you're not making progress.




SAY 'SIEM' AGAIN
I DARE YOU
memegenerator.net

https://v.gd/defenseAtScale10

SIEMs don’t detect compromises.

A human going “huh, weird”
detects a compromise.

some of the data
you collect

Increasing the hay stack does not make it easier to find the needle.

compromise
indicator

you

Lead by example.

Engineer: “Hey, can we add the new service account ‘fishbone’ everywhere? Needs full sudo, no password.”

Infosec: “LOL what? No way.”

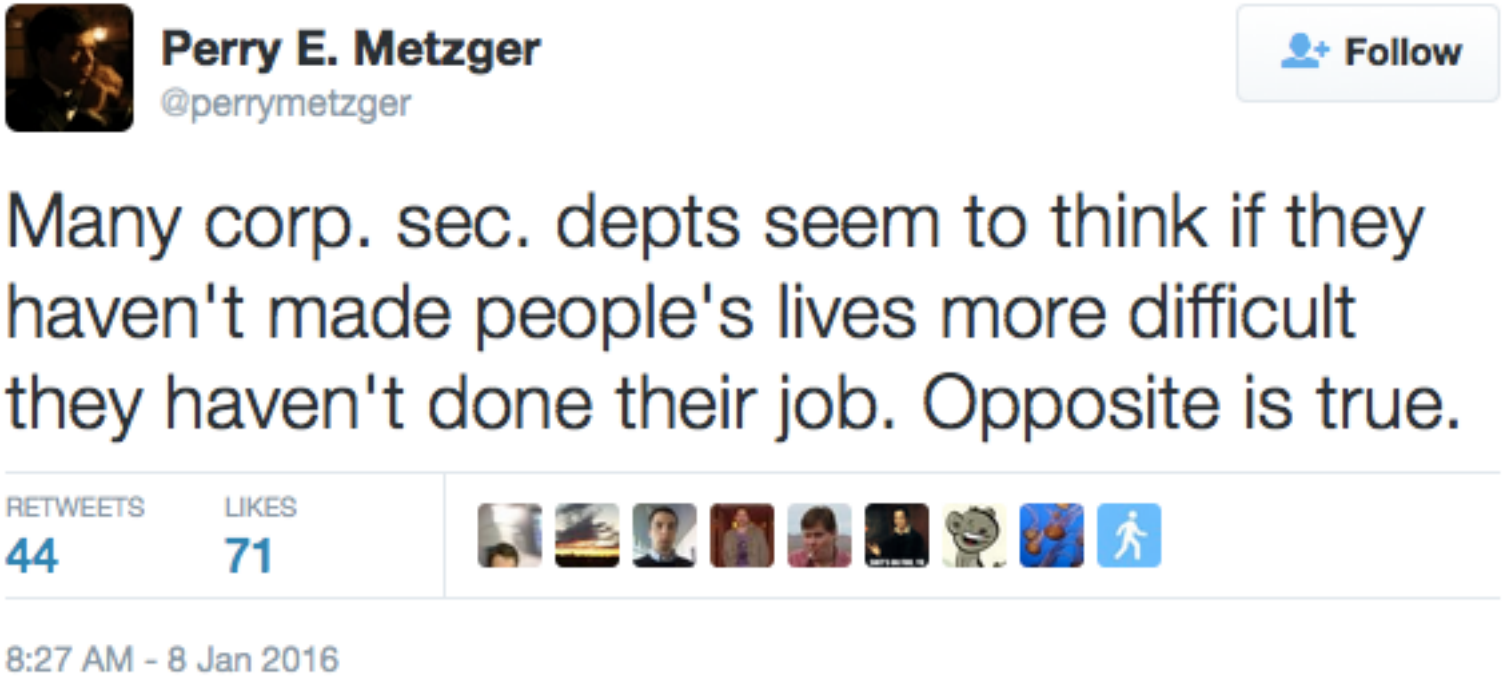
Infosec eng1: “Hey, can we add ‘nessus’ everywhere? Needs full sudo, no password.”

Infosec eng2: “Sure, one sec.”

Lead by example.

If another team asked you, would you say ’no’?

Other people’s fucks are also limited.



https://v.gd/defenseAtScale11

Vulnerabilities are dense.

CI/CD is your friend.

Embrace automation.

CI/CD is your friend.

- You *cannot* update individual systems; you *can* ensure all your systems regularly get all updates automatically.

- You *cannot* remove individual vulnerabilities; you *can* gate deployments on using the right libraries.

- You *cannot* manually change a config file on a few hundred thousand systems; you *can* enforce consistent convergence in idempotent changesets prescribed by your configuration management system.

Your endpoint security model should assume the network is compromised; your network security model should assume the endpoint is.

Both in fact are.

Consider today:

- auto-update your OS, third-party- and custom software
- mandatory configuration management across your fleet
- 2FA SSO with time-bound authentication tokens
- provide libraries for common problems (secret management, input/output validation, hashing, encrypting, ...)
- have exactly one TLS stack that everybody uses (internally and externally)

…and what may come:

- Embrace the cloud. You are already operating in hostile networks and crossing trust boundaries.

- Rethink your ‘trusted network’ (*BeyondCorp*).

- Rethink the need for user accounts.

https://v.gd/defenseAtScale13

…and what may come:

- Containers are just big ass static binaries with all their problems. Deal with it.

- Build upon remote attestation of both hardware and software; signed containers.

Defend smarter, not harder.

- Don't waste your time on busy work. Measure your impact. Prioritize.
- Embrace automation. Move fast.
- Help others take responsibility. Guide them.
- Have a Red Team.
  "You can't grade your own homework."
  – @MicahZenko

Thanks!

BSidesNYC

2016

https://v.gd/defenseAtScale

Jan Schaumann

@jschauma