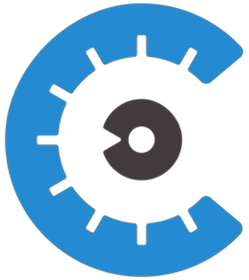


DevOps Is Automation, DevSecOps Is People

(ISC)² Security Congress

Mike Shema
@CodexWebSecurum

October 10, 2018

“No one knows who they were or what they were doing.”

–*Nigel Tufnel,* This is Spinal Tap

DevOps

Automation	Required to scale. Establishes consistency. Enables confident iteration.

Dev[Sec]Ops

People

Working with them.

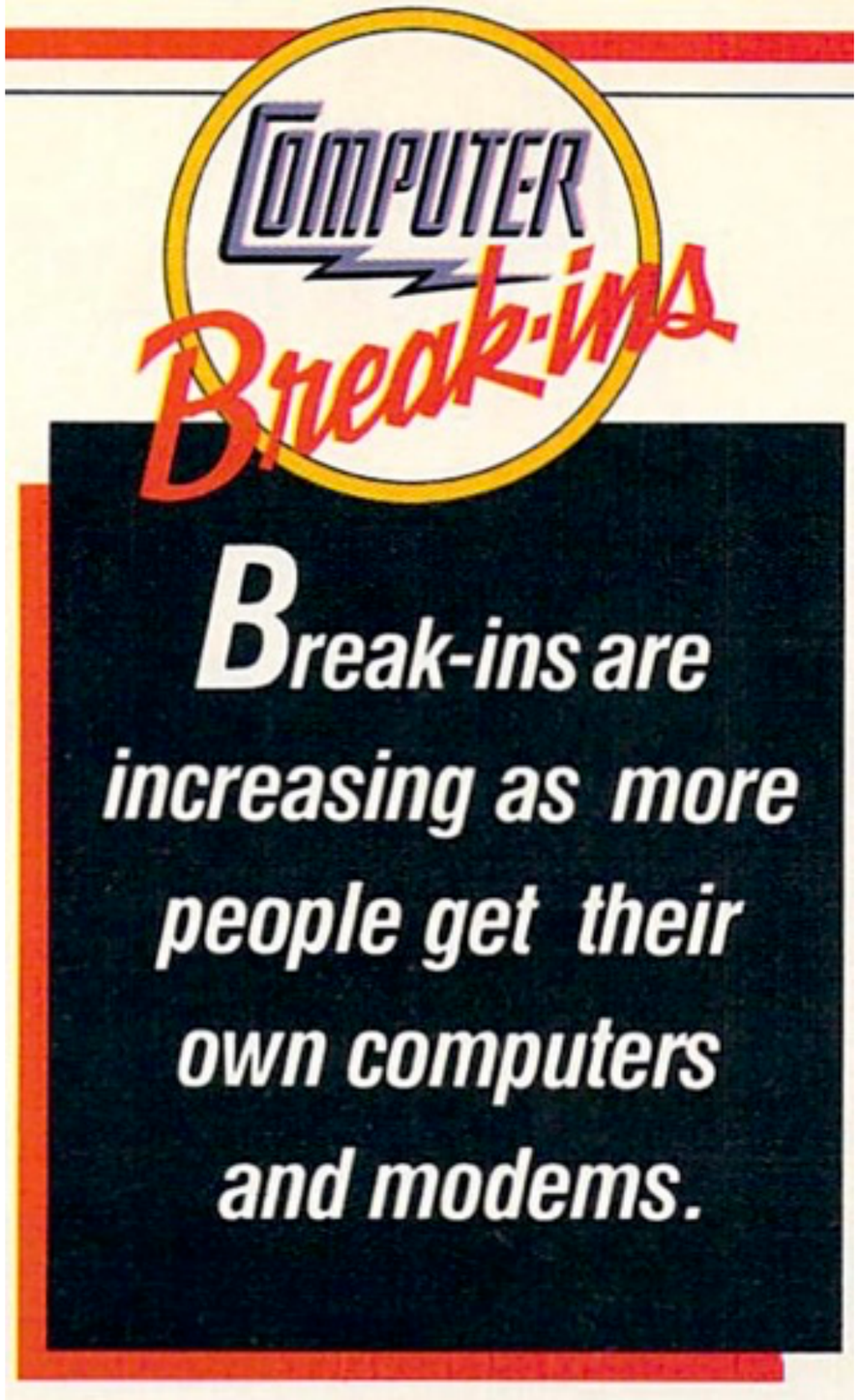
Working for them.

Building for them.

“I don't wanna bust out of here and find nothing but a lot of cold circuits waiting for me.”

–*Tron,* TRON

Welcome to the 1980s

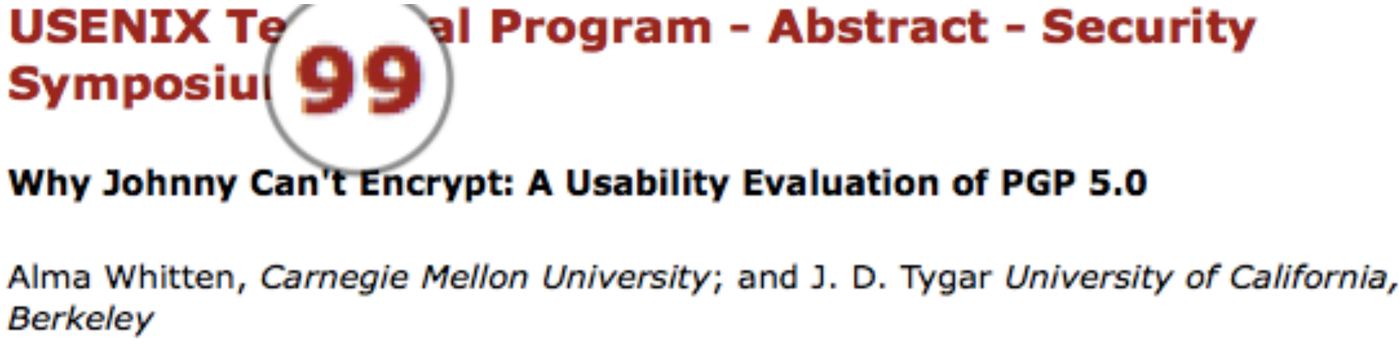


Actual Problem Ignored

Users are stupid.

Devs are lazy.

Vuln equals risk.



USENIX Te al Program - Abstract - Security Symposiu 99

Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0

Alma Whitten, *Carnegie Mellon University*; and J. D. Tygar *University of California, Berkeley*

https://www.usenix.org/legacy/publications/library/proceedings/sec99/whitten.html

Fantasy Campaign Setting

Race	Penalty or Bonus
Dwarf	Constitution +1; Charisma -1
Elf	Dexterity +1; Constitution -1
Half-Orc	Strength +1; Constitution +1; Charisma -2
Halfling	Strength -1; Dexterity +1
User	Intelligence -2; Wisdom -2
Developer	Intelligence -2; Wisdom -2

Monstrously Manual

Key rotation is a critical to usable encryption.

Move security to where the devs are.

Let’s Encrypt addresses initial cost and ongoing maintenance.

Answers

CAN YOU TALK LIKE A HACKER?

Shared Vocabulary

Communication

Empathy

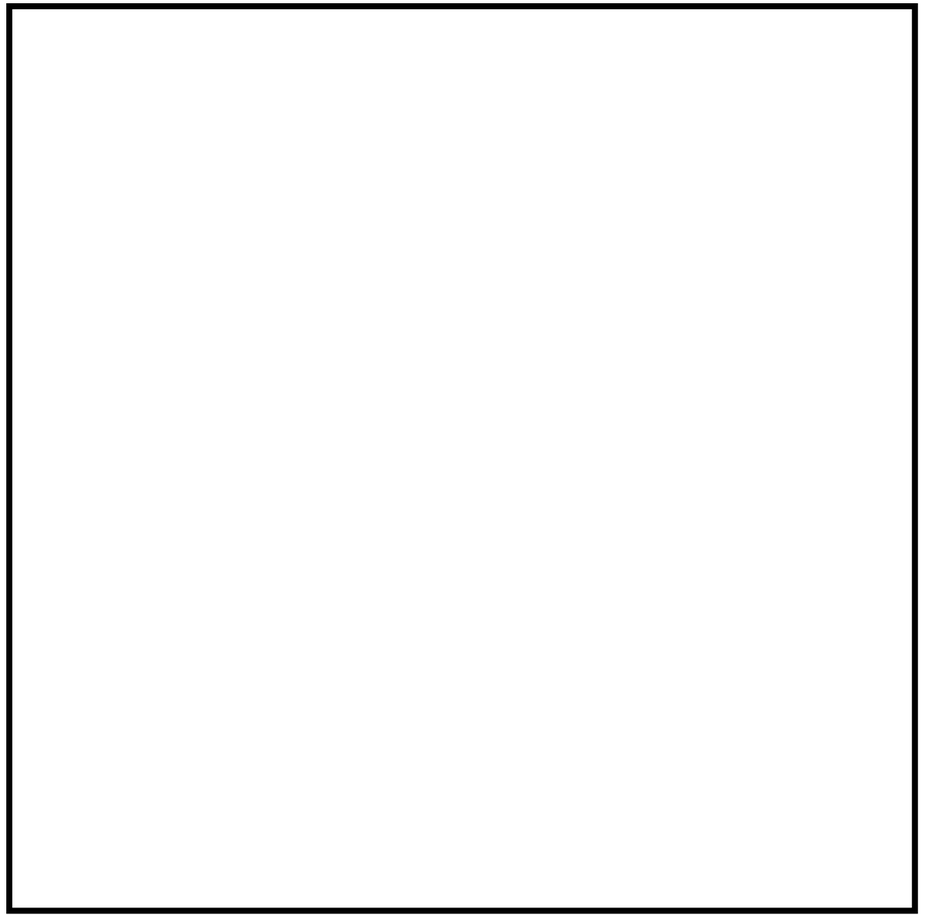
Threats

Communication

Listen

Acknowledge

Repeat back

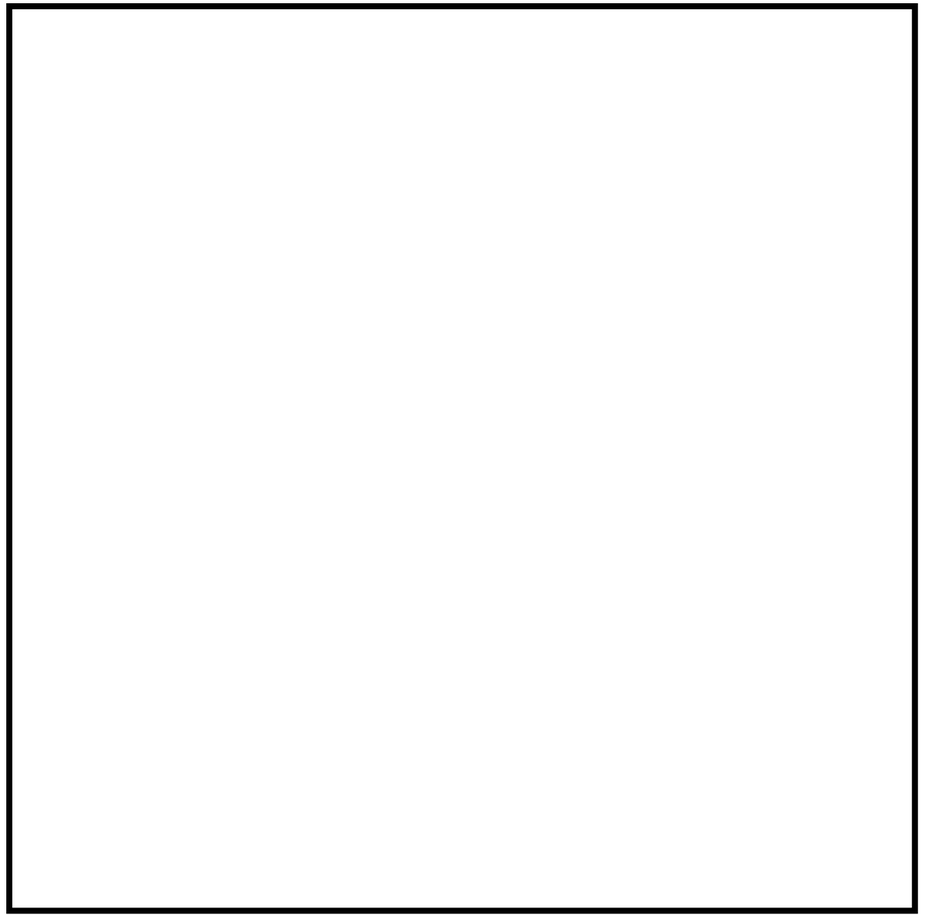


Empathy

Broaden understanding

Reconsider viewpoints

Improve solutions



Threats

Ambiguity

Erasure

Essentialization

Tabletop role-playing games

Collaborative story-telling

Communication exercise

Barbarian	Coder, Sysadmin
Fighter	DevOps
Magic-User	DevOps at scale
Thief	Red Team
Cleric	Blue Team
Ranger	Threat Hunting
Bard	CISO

RPG Interpersonal Skills

Compromise

Negotiation

Patience

Team-building

Personality (d8, d8)

1-5 Average	6-7 Extroverted	8 Introverted
1. modest	1. forceful	1. retiring
2. egoist/arrogant	2. overbearing	2. taciturn
3. friendly	3. friendly	3. friendly
4. aloof	4. blustering	4. aloof
5. hostile	5. antagonistic	5. hostile
6. well-spoken	6. rude	6. rude
7. diplomatic	7. rash	7. courteous
8. abrasive	8. diplomatic	8. solitary/secretive

Disposition (d10)

1. cheerful
2. morose
3. compassionate/sensitive
4. unfeeling/insensitive
5. humble
6. proud/haughty
7. even tempered
8. hot tempered
9. easy going
0. harsh

Captain Awkward

Terminology

Shared vocabulary

References

https://captainawkward.com

RPG Threat Models

Rolling for initiative.

Splitting the party.

Touching the statue.

Attacking the darkness.

Attacking the Darkness

Ambiguity in design.

Not perceiving a threat model.

Assuming a uniform user.

A Fiendish Folio

Abuse

Distributed abuse

Less sophistication

Less access to technology

Privacy*

*Summons 2d6 more privacy demons

More Than Denial of Service

Asymmetric effort (time) costs, e.g. 100 people sending a DM, 1 person deleting 100 DMs.

Asymmetric attention (time) costs, e.g lack of filters, lack of mass changes.

More Than Code Execution

Ratings without context or with irrelevant context.

Reputational damage. Reputational abuse.

Involuntary participation, added to list of X, added to repo of Y.

More Than Escalation

Metadata leaks, when is user active.

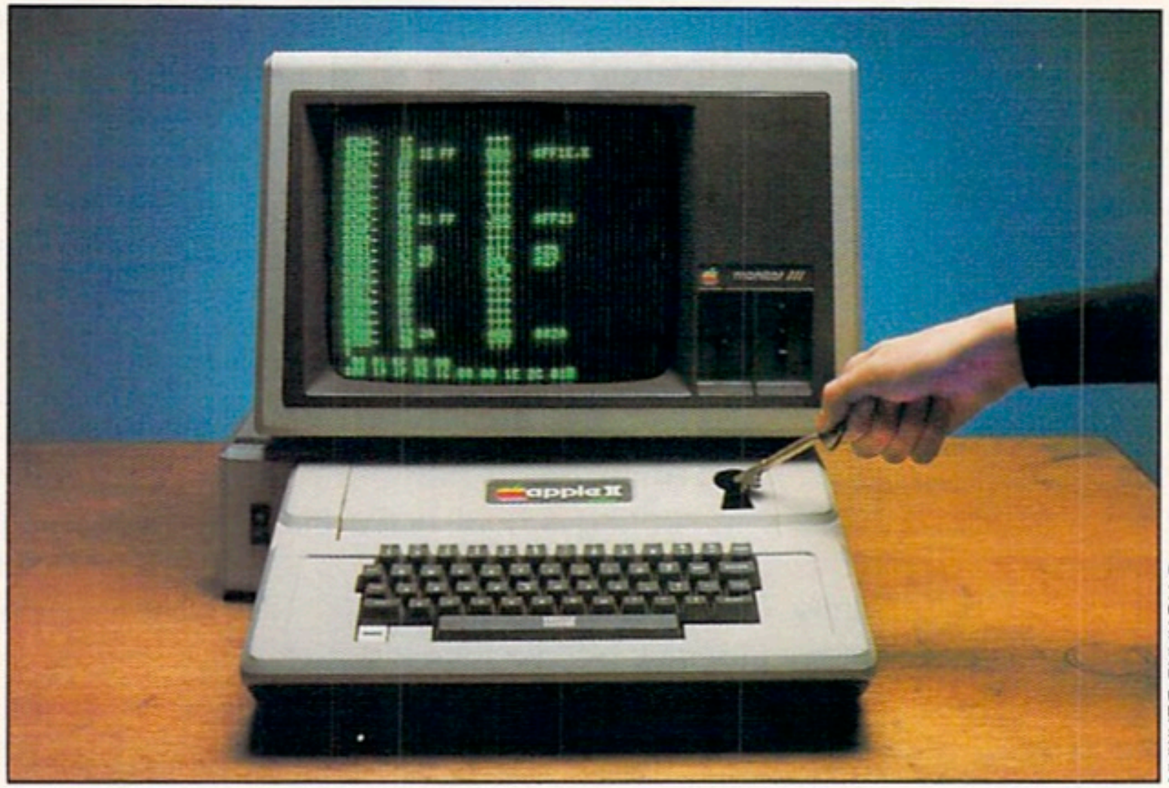
De-anonymization of identity, de-aggregation of cohorts.

Lack of personas.

Security (or privacy) as a cost.

How Break-Ins Happen

And How They're Being Stopped



Build a Story (Cautiously)

Ask an interesting question.

Collect signals, beware silence.

Create metrics, beware tunnel vision.

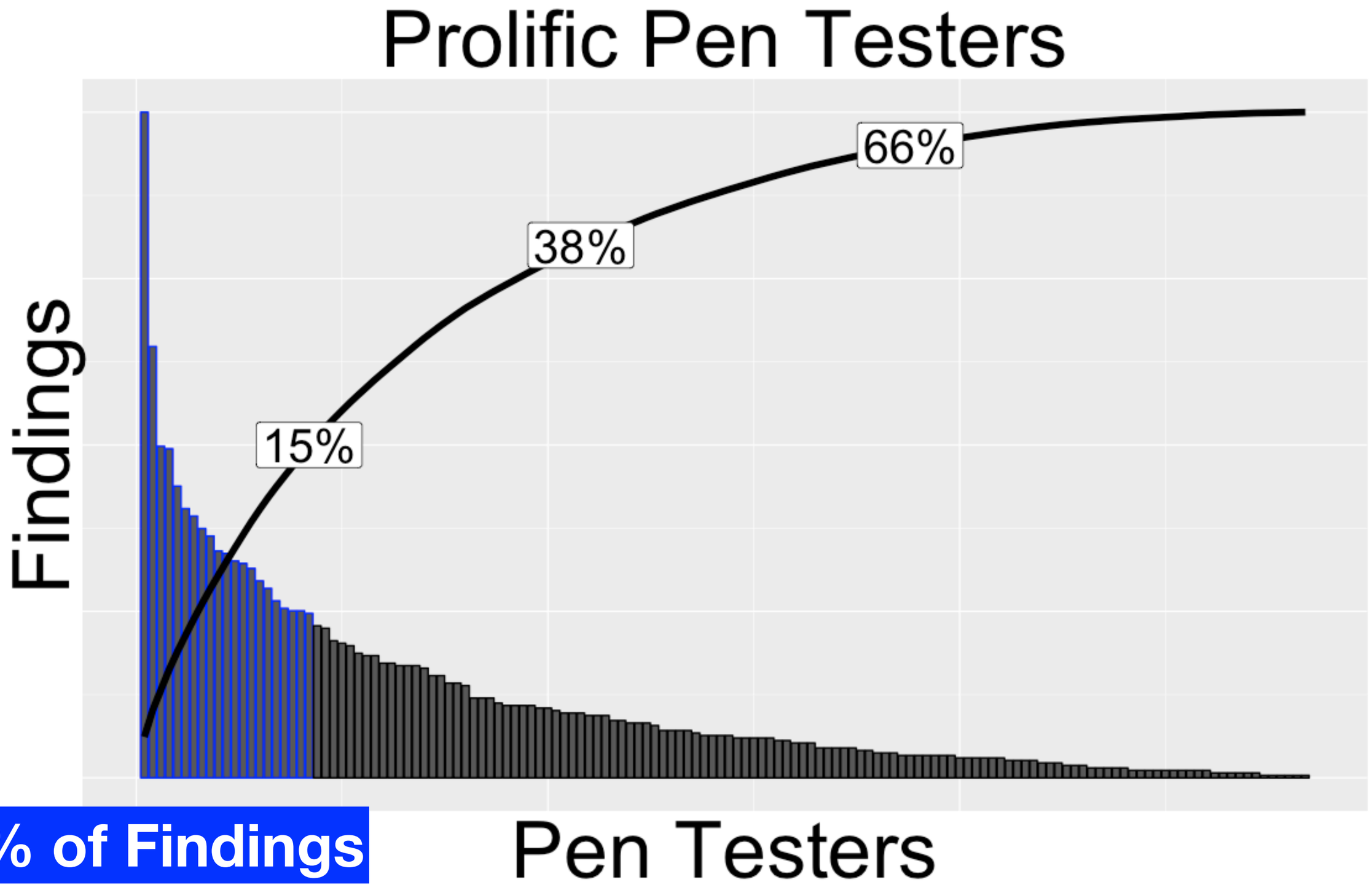
Create a story, beware myth.

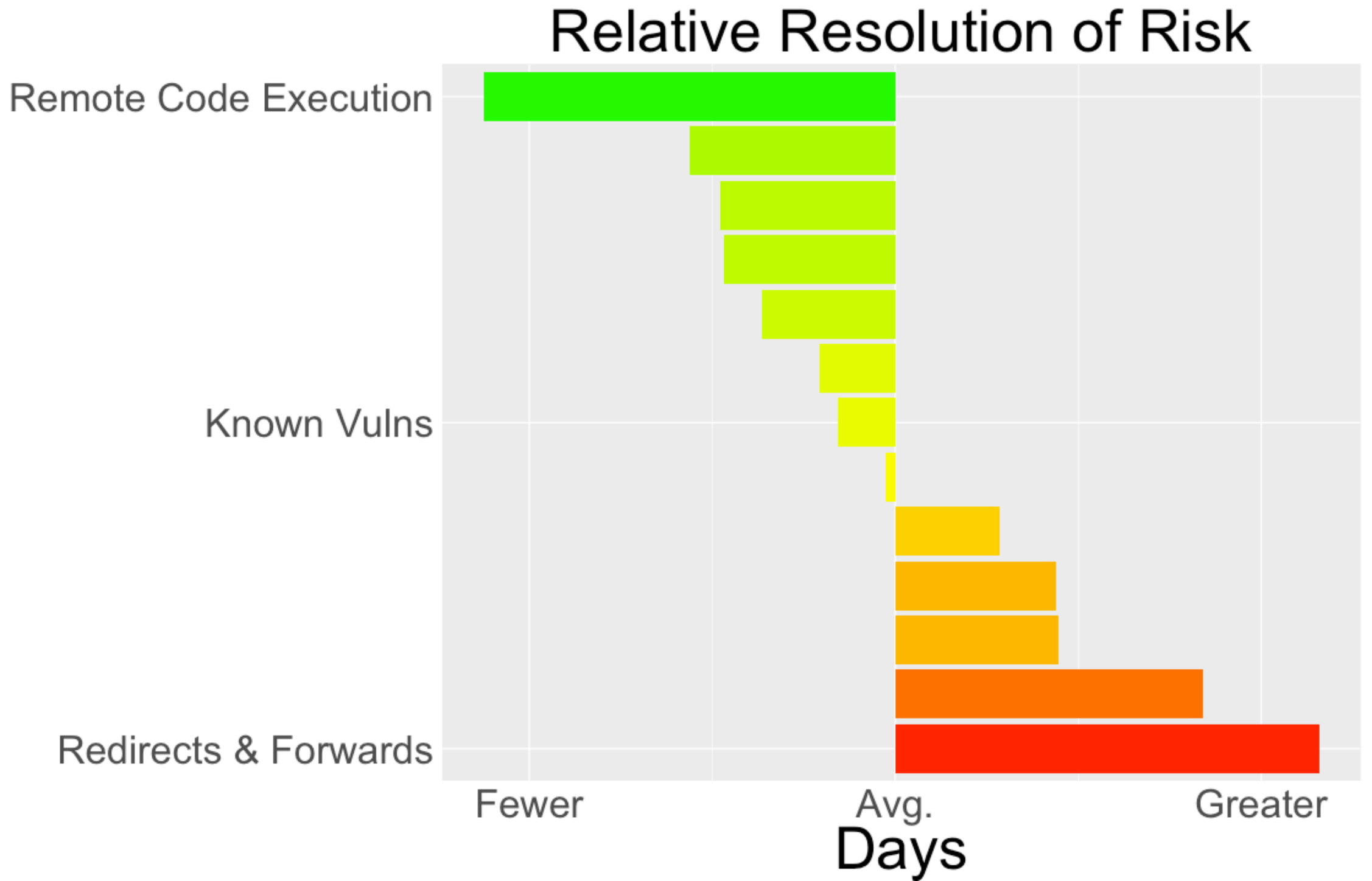
CI/CD for Metrics

Attain a goal, don’t manage a number.

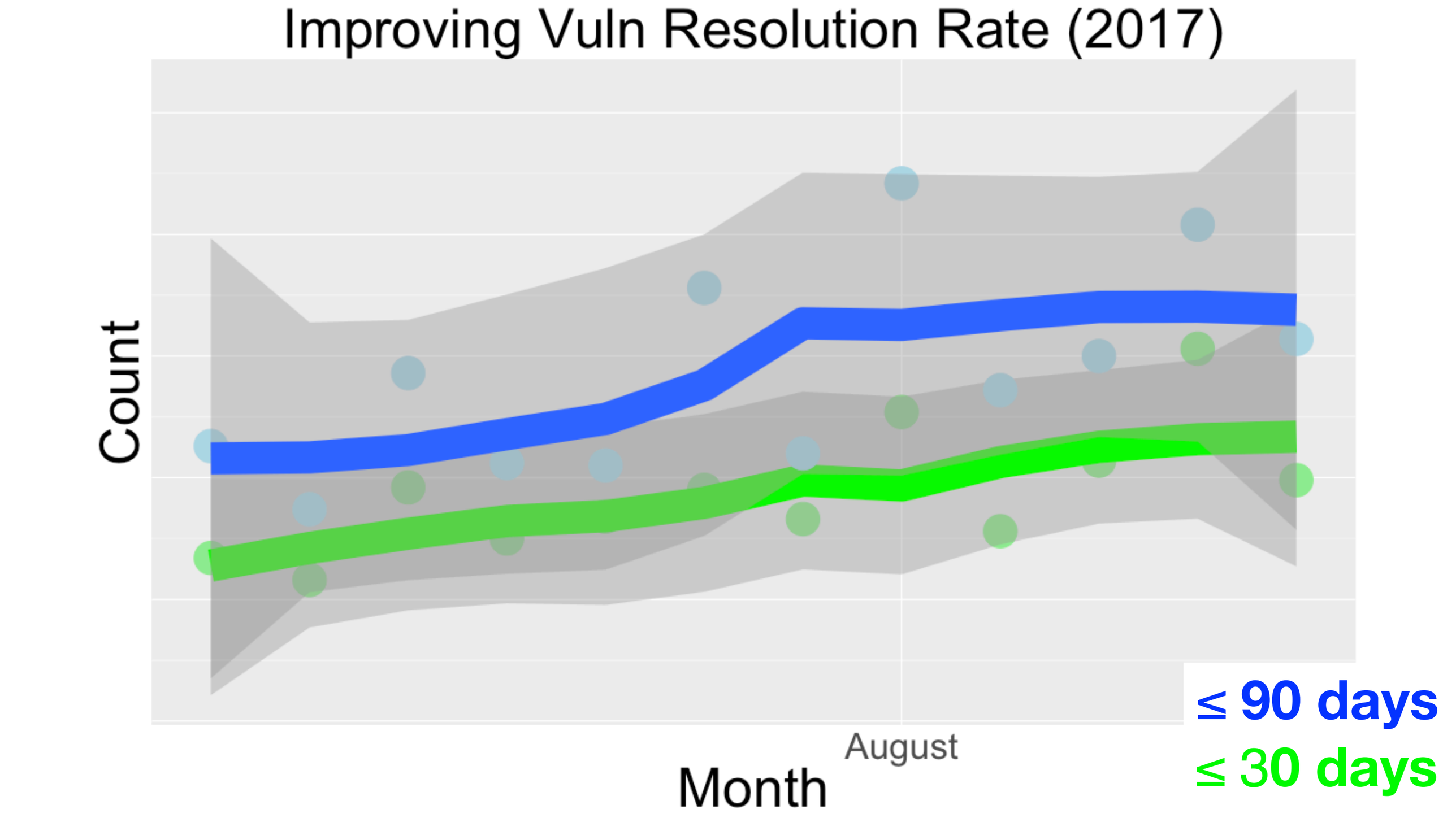
Review and revise based on feedback.

Watch for unintended consequences.


Prolific Pen Testers
Findings
15%
38%
66%
Pen Testers
50% of Findings


Relative Resolution of Risk
Remote Code Execution
Known Vulns
Redirects & Forwards
Fewer
Avg.
Greater
Days


Steps to Security
24%
Number of Orgs
Few
Half
All
Amount of Vulns Resolved


Improving Vuln Resolution Rate (2017)
Count
August
Month
≤ 90 days
≤ 30 days

Threats

Lack of signals

Unrepresentative signals

Tunnel vision

Information bias

Unearthing Arcana

What we measure also reflects what we care about.

What we care about also reflects on our environment.

BOY-GIRL RATIO	HARDWARE, CAMPER-COMPUTER RATIO	LANGUAGES TAUGHT	TYPE OF INSTRUCTION, HOURS PER DAY
3:1	Atari computers, 2:1 ratio	BASIC, PILOT	Instructors have computer teaching backgrounds. All camps ACA.**
3:2	Apple II, Atari, Commodore 64, IBM, Radio Shack, Texas Inst., 1:1 ratio	Assembly, BASIC, LOGO, Pascal	Instructors have teaching and computer background. 7 out of 9 locations. ACA**
2:1	Apple II, IBM PC, 2:1 ratio	BASIC, LOGO, Pascal	Instructors have teaching and computer backgrounds.
5:1	Apple IIe, TRS-80, 2:1 ratio	Assembly, BASIC, Pascal	Instructors have teaching backgrounds.
4:1	Apple II, Commodore 64, 1:1 ratio	Assembly, BASIC, Forth, LOGO, Pascal	Instructors are computer science grads and undergrads. All camps ACA.**

Children's Television Workshop, Enter Magazine, March 1984

Threats—Cognitive Biases

Bandwagon

Choice-supportive

Clustering illusion (vulns…)

Confirmation bias

Information bias (numbers, metrics)

Stereotyping

DevSecOps Is People

Remember

who implements features.

who benefits from them.

social dimensions in your threat models.

“War is the continuation of politics by other means.”

–*Carl von Clausewitz,* On War

“AppSec is the continuation of DevOps by their own means.”

Made **by** people

Made **for** people

Made **of** people

Thank You!

End of line.

Questions?

@CodexWebSecurum

More Resources

https://captainawkward.com

http://www.crashoverridenetwork.com

http://geekfeminism.wikia.com/wiki/Category:Concepts

https://tallpoppy.io