DevOps Is Automation, DevSecOps Is People

OWASP AppSec Cali

Mike Shema
mike@cobalt.io

January 30, 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

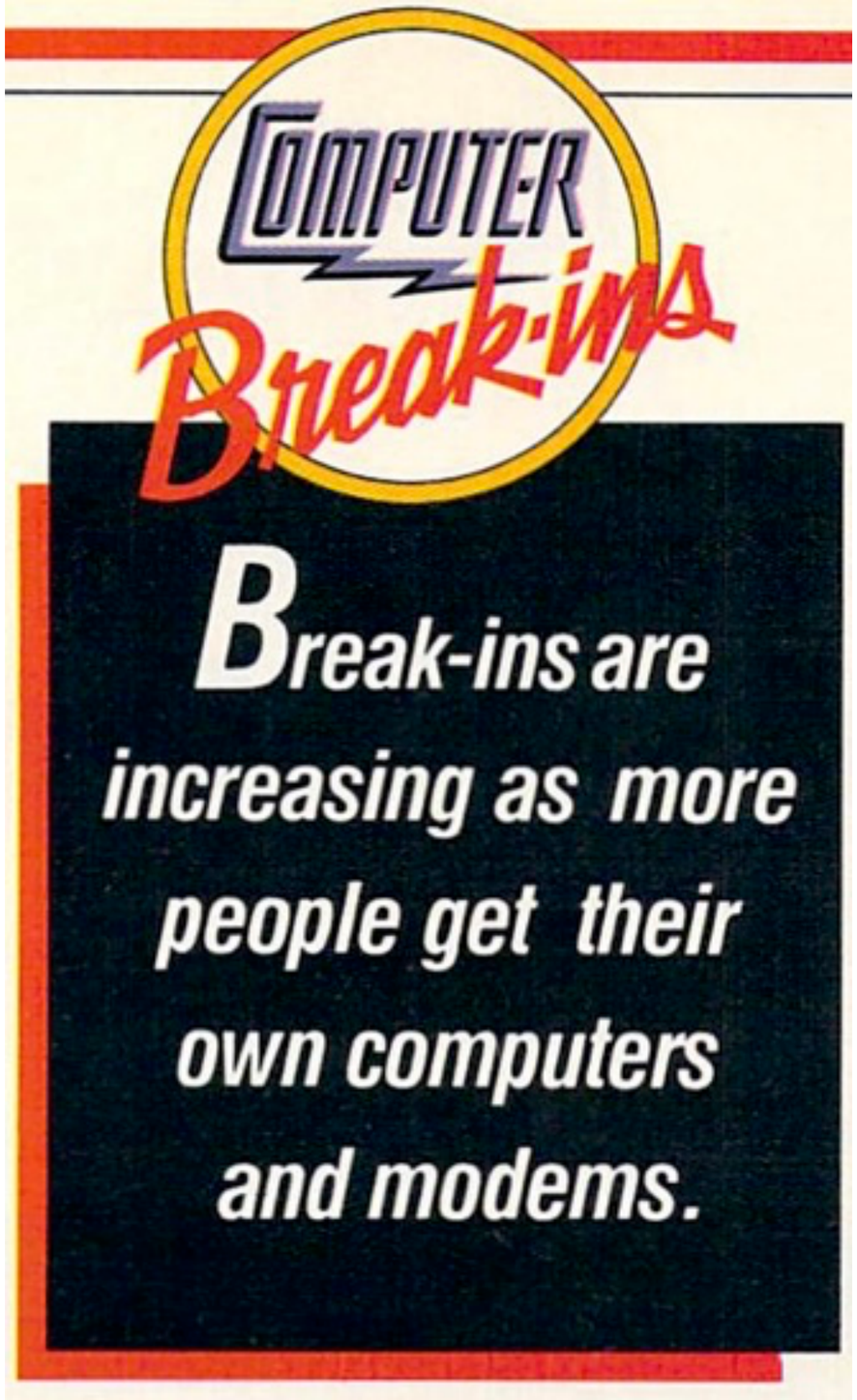
Building for them.

Working for them.

Working with them.

Make Room! Make Room!

Welcome to the 1980s



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

–*Tron,* TRON

Made by people

Made for people

Made of people

Soylent

Soylent

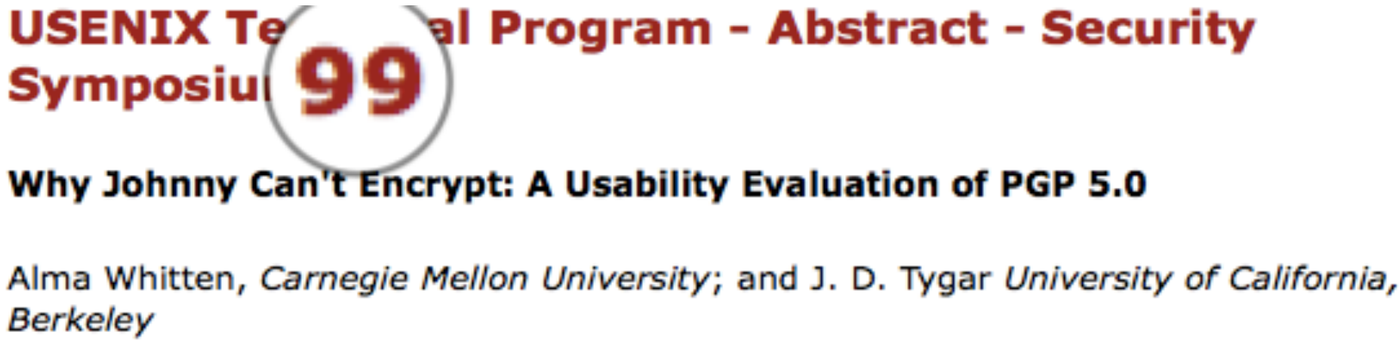
Soylent

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*

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

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

–*Carl von Clausewitz,* On War

CI/CD Pipeline

Rearranges security boundaries.

Provides touchpoints for security checks.

Enables actions for security feedback.

Shared Vocabulary

Communication

Empathy

Action

Feedback

Communication

Answers

CAN YOU TALK LIKE A HACKER?

Children's Television Workshop, Enter Magazine, October 1983

Risks

Ambiguity

Erasure

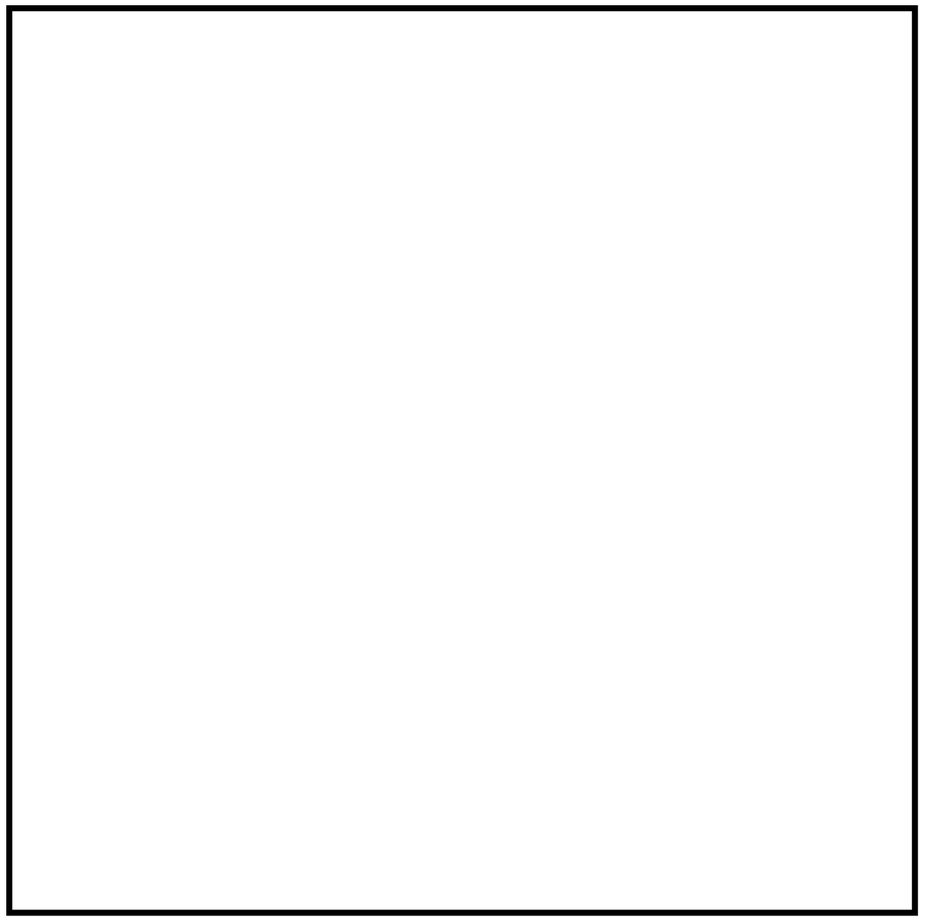
Essentializing

Empathy

Listen

Acknowledge

Repeat back



Codes of Conduct

Set expectations, standards of behavior.

Describe a path for conflict resolution, define consequences.

Foster participation.

Example: https://golang.org/conduct

Tabletop role-playing games

Collaborative story-telling

Communication exercise

Class of Character

CAVALIER
- Paladin

CLERIC
- Druid

FIGHTER
- Barbarian
- Ranger

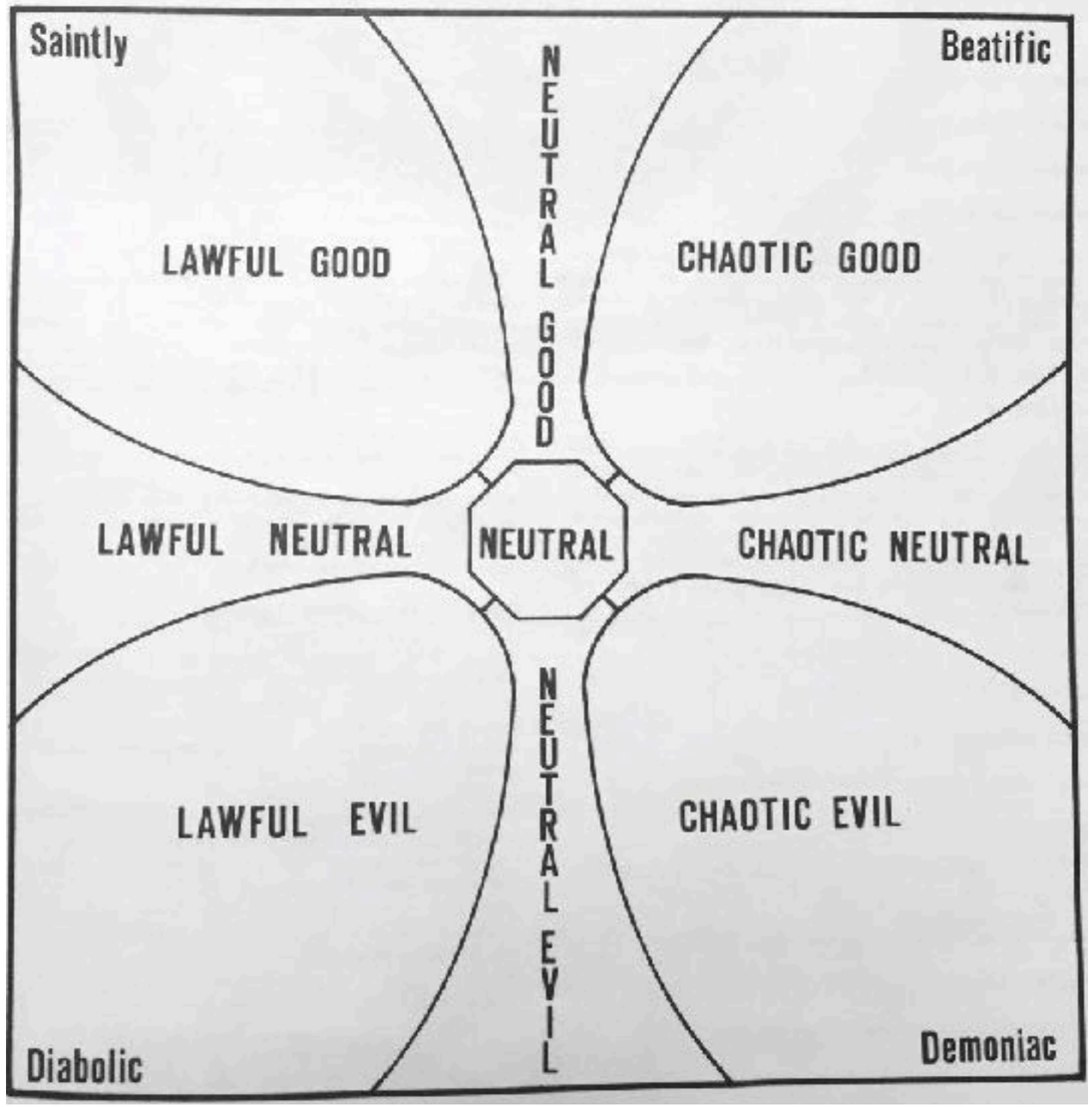
MAGIC-USER
- Illusionist

THIEF
- Acrobat
- Assassin

MONK

BARD

APPENDIX III: CHARACTER ALIGNMENT GRAPH



Lists

Tables

Appendices

More tables

Dice

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

Threat Modeling

TABLE V. I.: TREASURE IS GUARDED BY (d20)

Die	Result
1-2	Contact poison on container
3-4	Contact poison on treasure
5-6	Poisoned needles in lock
7	Poisoned needles in handles
8	Spring darts firing from front of container
9	Spring darts firing up from top of container
10	Spring darts firing up from inside bottom of container
11-12	Blade scything across inside
13	Poisonous insects or reptiles living inside container
14	Gas released by opening container
15	Trapdoor opening in front of container
16	Trapdoor opening 6' in front of container
17	Stone block dropping in front of the container
18	Spears released from walls when container opened
19	*Explosive runes*
20	*Symbol*

RPG Threat Models

Splitting the party.

Attacking the darkness.

Touching the statue.

Rolling for initiative.

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

Legends & Lore

Breach

Weak password choice?

Weak hashing algorithm?

Weak architecture?

A Fiendish Folio

Abuse

Distributed abuse

Less sophistication

Less technology availability

Privacy*

*Summons 2d6 more privacy demons

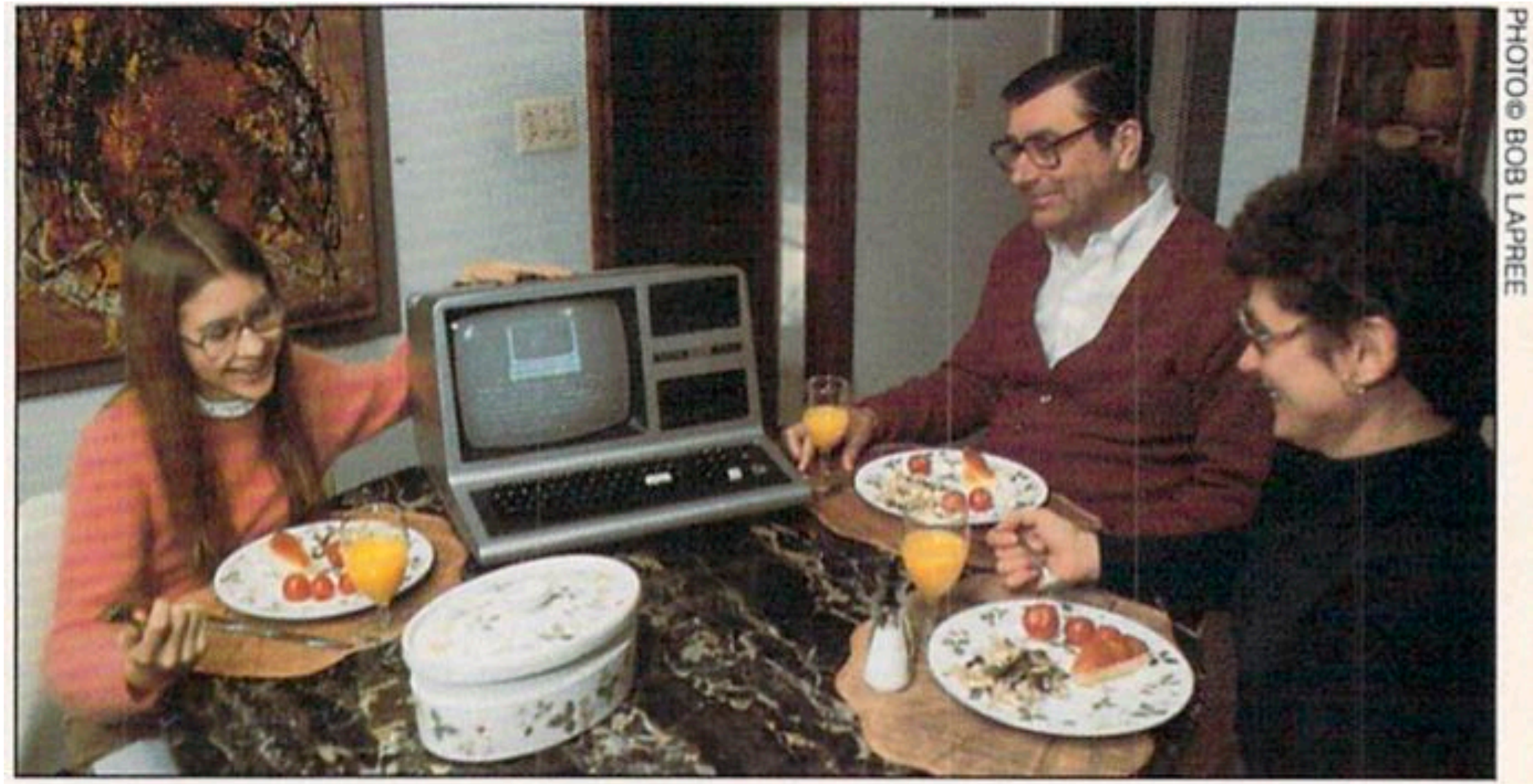
Monstrously Manual

Let’s Encrypt addresses cost and time.

Key rotation is a critical to usable encryption.

Observe and Measure

Weary of Awareness



Parents can be taught to use computers—but it takes time.

Children's Television Workshop, Enter Magazine, March 1984

Meaningful Metrics

Attaining a goal vs. managing a number.

Review, revise, reveal unintended consequences.

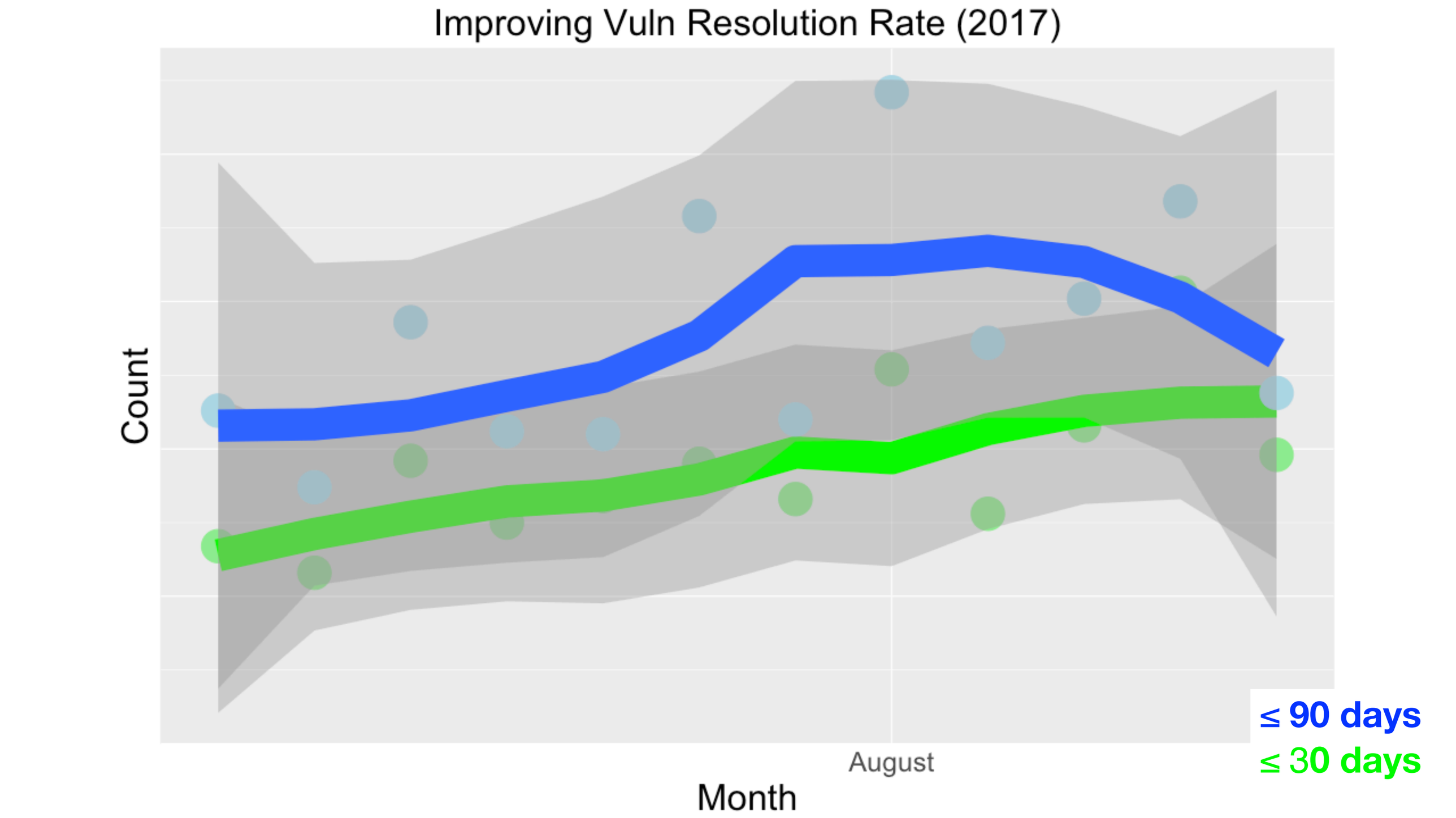
Improving Fix Verification

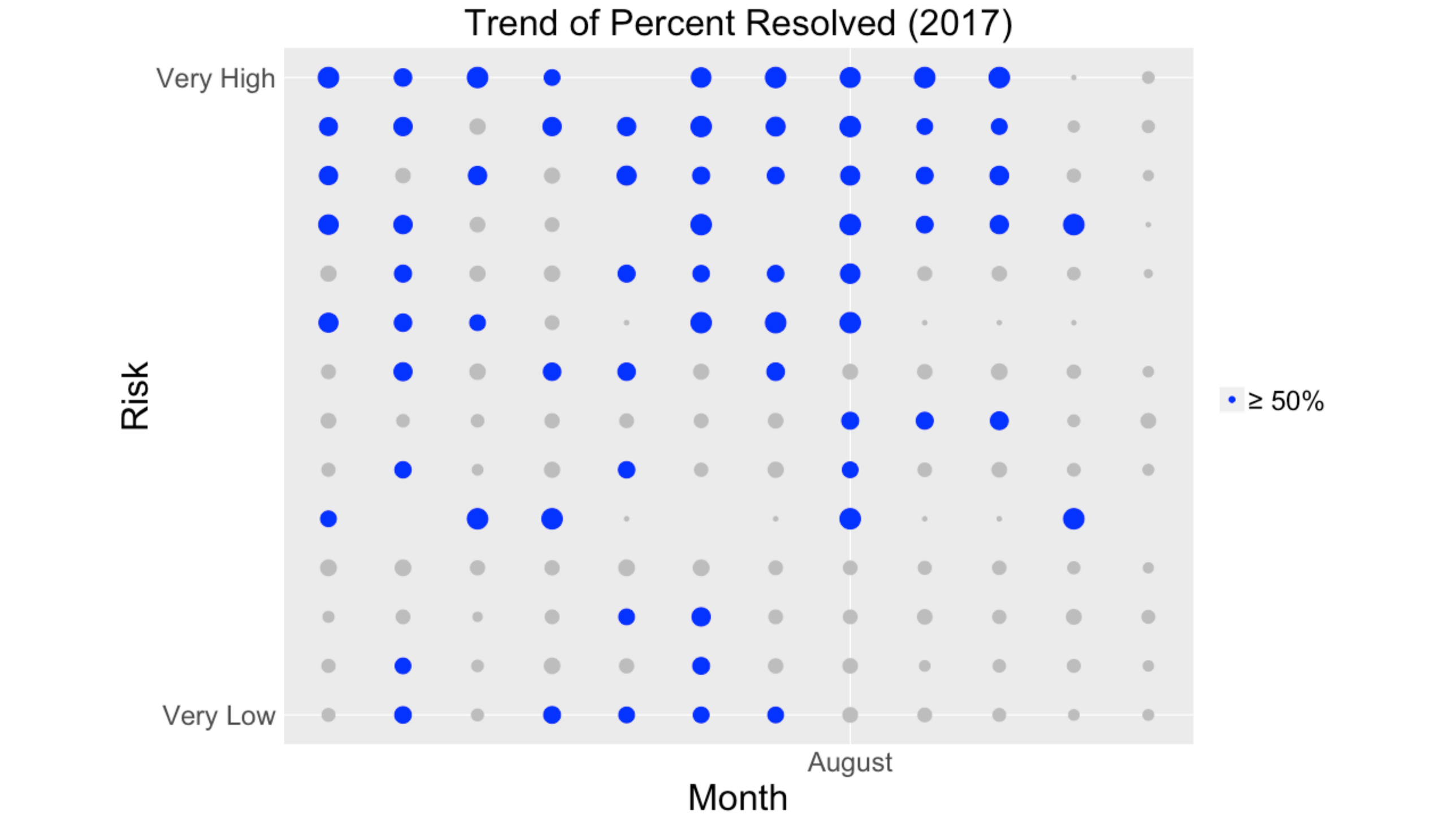
Verifying fixes was slow, ad-hoc.

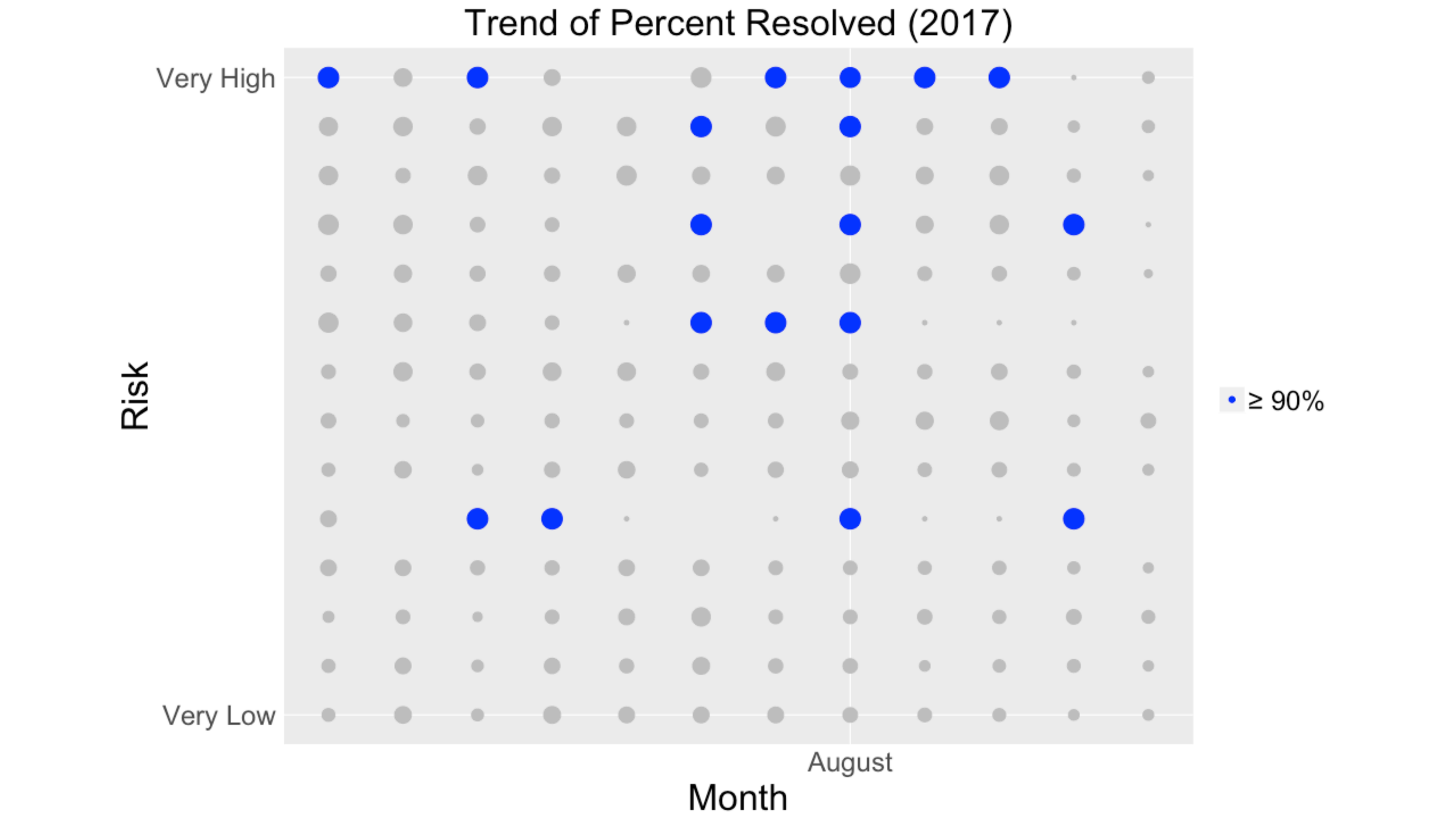
Couldn’t track time of state transitions.

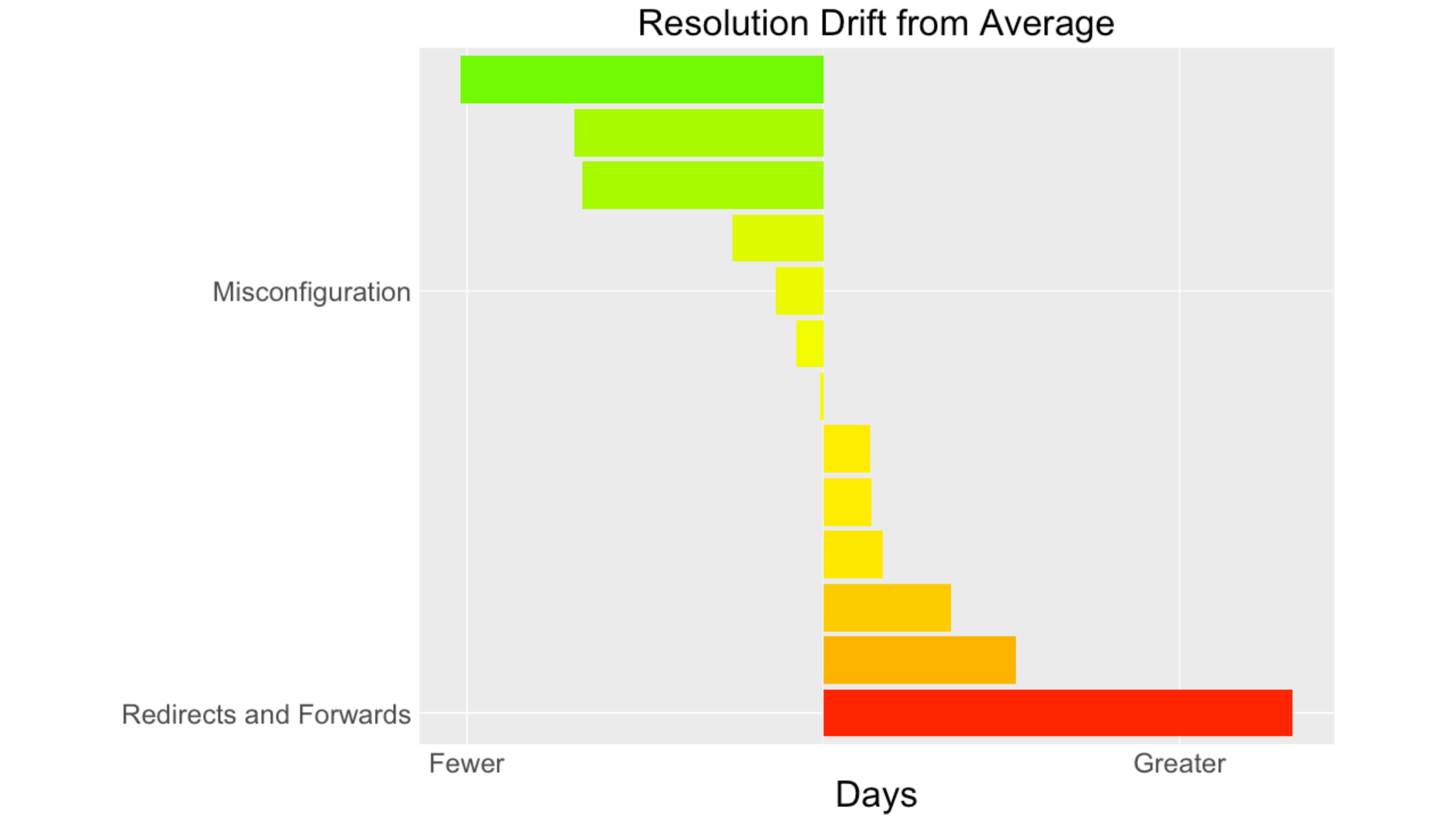
Notifications weren’t prioritized.

We’re doomed.


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


Trend of Percent Resolved (2017)
Very High
Very Low
Risk
August
Month
≥ 50%


Trend of Percent Resolved (2017)
Very High
Very Low
Risk
August
Month
≥ 90%


Resolution Drift from Average
Misconfiguration
Redirects and Forwards
Fewer
Greater
Days

Surface salient information

Set attainable goal

Communicate plan, importance

Query for challenges

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

Manual of the Planes

What are you measuring? How are you measuring?

Are you choosing a metric only because it’s available?

Cognitive Biases

Bandwagon

Choice-supportive

Clustering illusion (vulns…)

Confirmation bias

Information bias (numbers, metrics)

Stereotyping

Mind Flayer

D&D continues to evolve.

Cliques, in-groups, and gate-keeping are threats to any social group.

Not everyone is familiar with it.

Tough 10(-ish) List

Account recovery

Password storage

Software dependency management

Anonymization

Abuse

Continuous Integration

Continue to press on identifying architectural security flaws, proposing technical solutions.

Remember who implements them.

Remember who benefits from them.

Continuous Deployment

Not just passive awareness. Active execution.

Meaningful understanding. Doesn’t need expertise, but shouldn’t be misapplied.

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

–Mike Shema

Thank You!

End of line.

Questions?

@CodexWebSecurum