OWASP AppSec EU Belfast

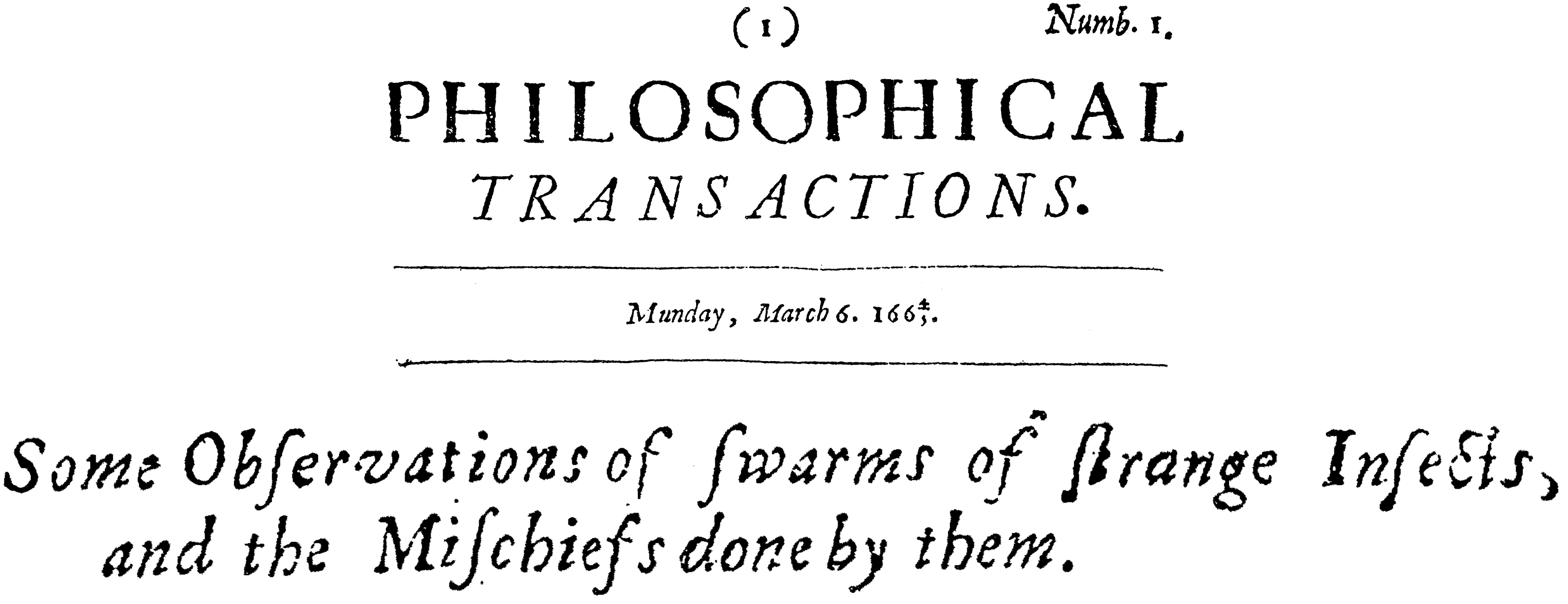
8th to 12th of May 2017

Waterfront Conference Center

The Flaws in Hordes, The Security in Crowds

OWASP AppSec EU
May 12, 2017

Mike Shema
mike@cobalt.io



Numb. 1.

PHILOSOPHICAL TRANSACTIONS.

Munday, March 6. 166$\frac{4}{5}$.

Some Obſervations of ſwarms of ſtrange Inſects, and the Miſchiefs done by them.

Some Observations of Swarms of Strange Insects, and the Mischiefs done by them.

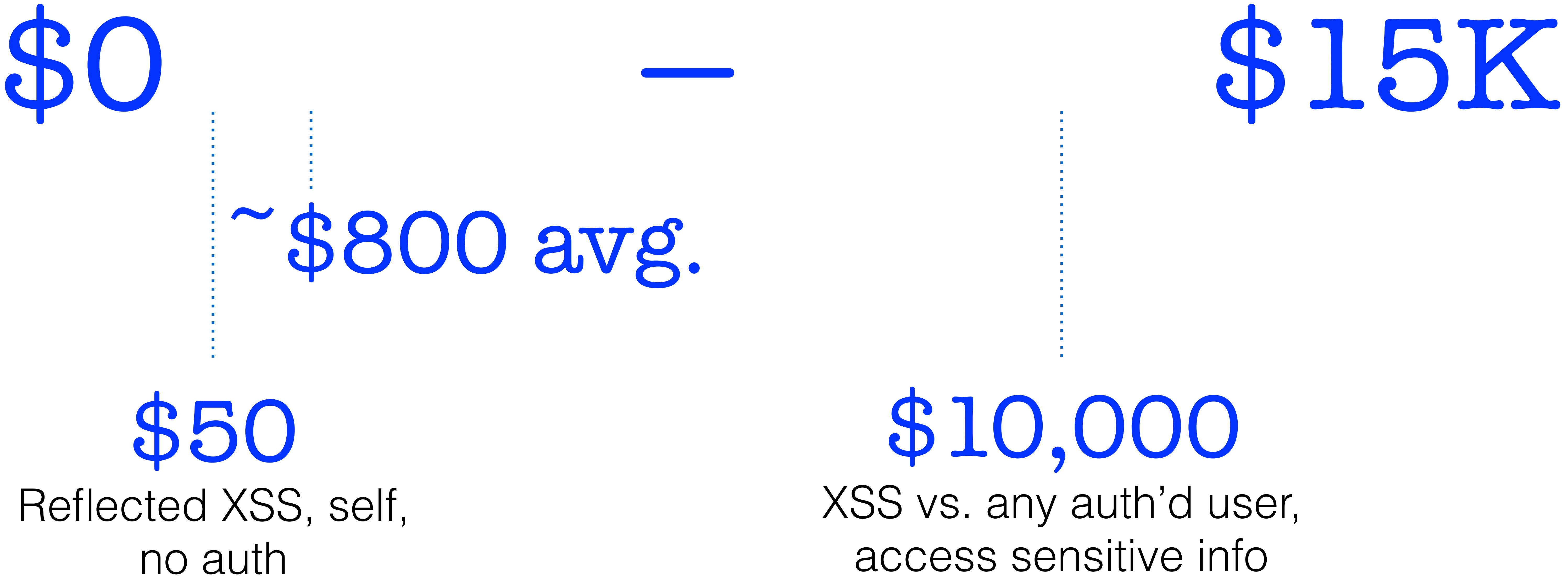
A **cacophony** of hordes.

A **scrutiny** of crowds.

How do we…

- find vulns efficiently?
- spend wisely?
- reduce risk?

Bounties are an imperfect proxy for risk, where price implies impact.



$0 — $15K

~$800 avg.

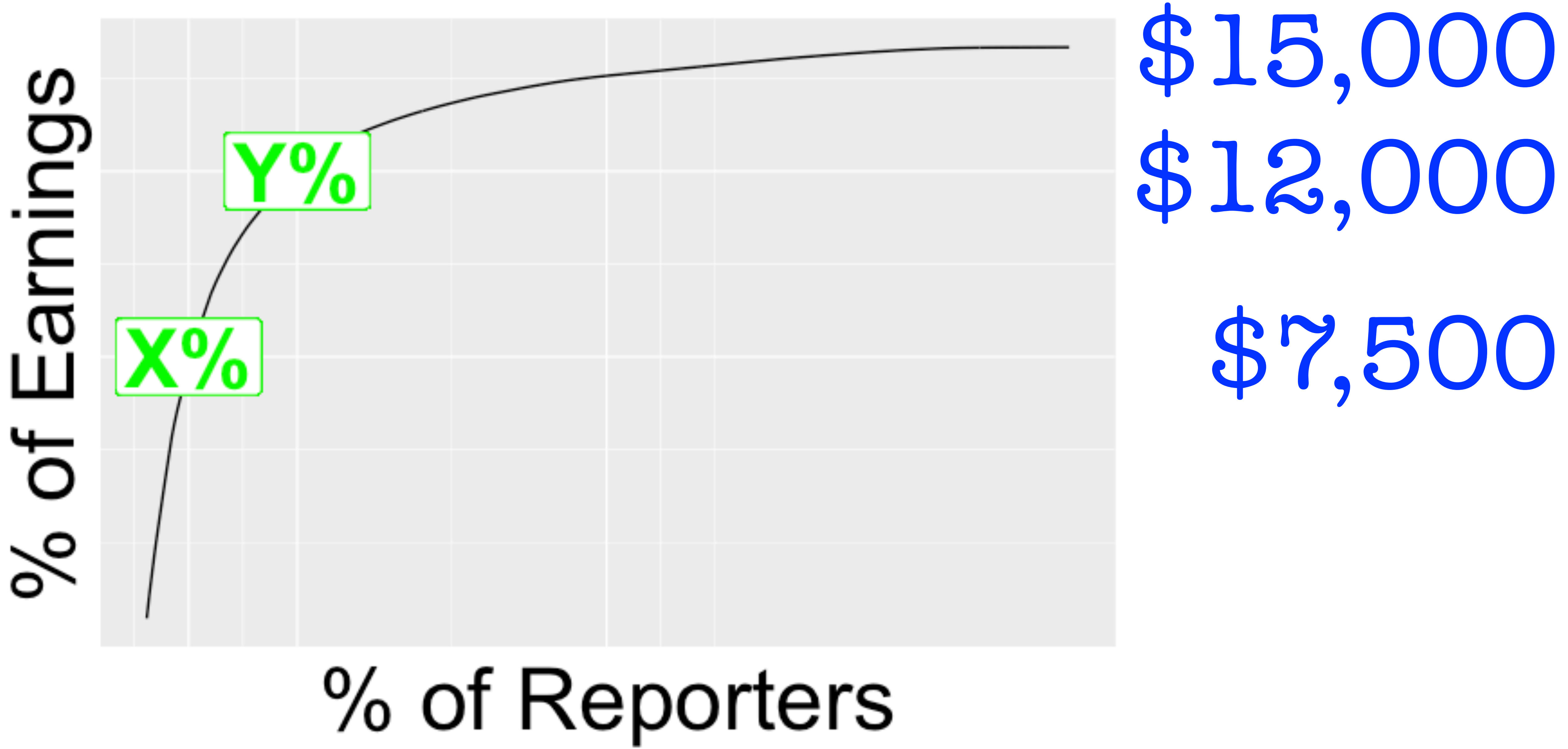
$50

Reflected XSS, self,
no auth

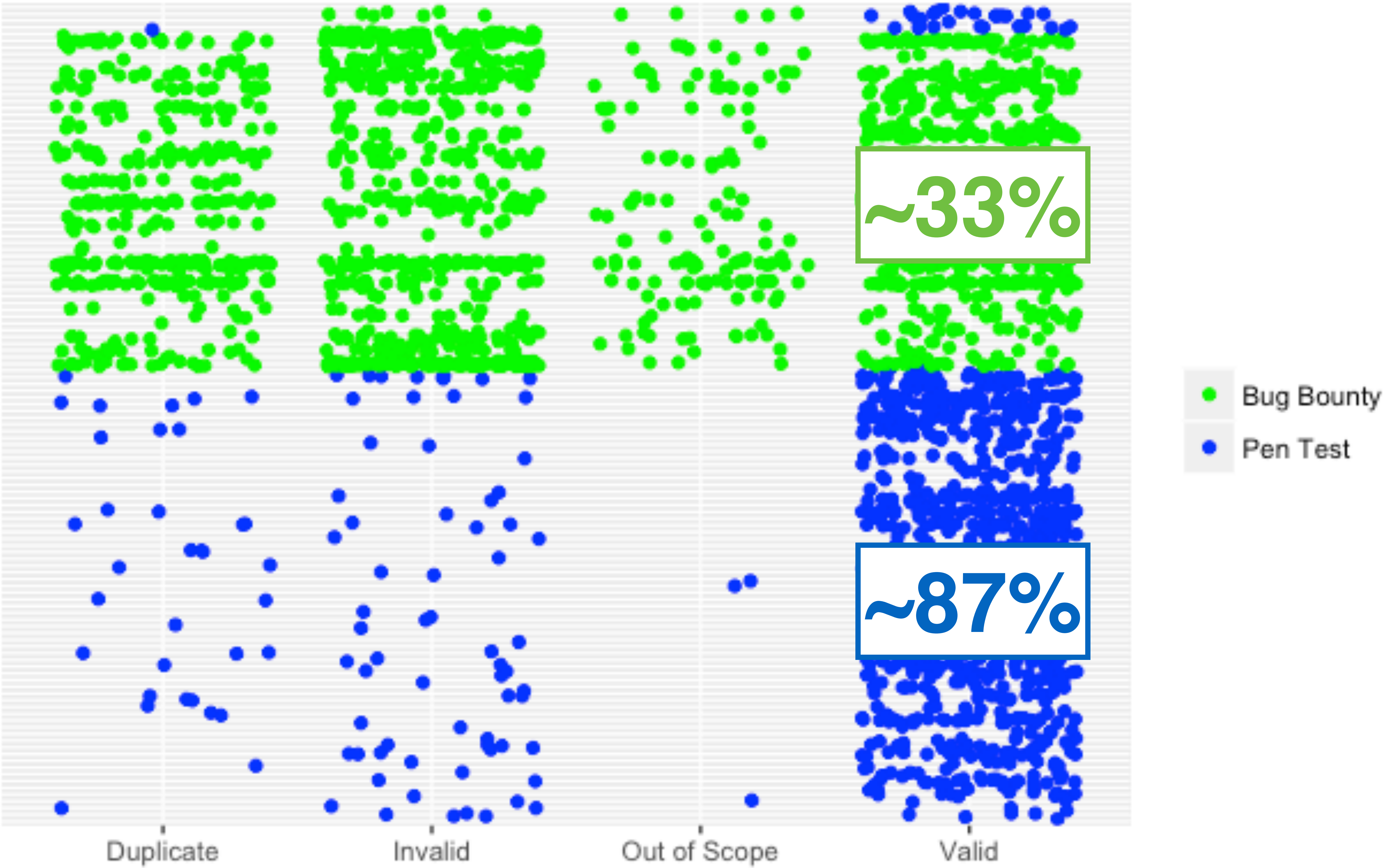
$10,000

XSS vs. any auth'd user,
access sensitive info

Bounties are an imperfect proxy for work, where earnings may diverge from effort.



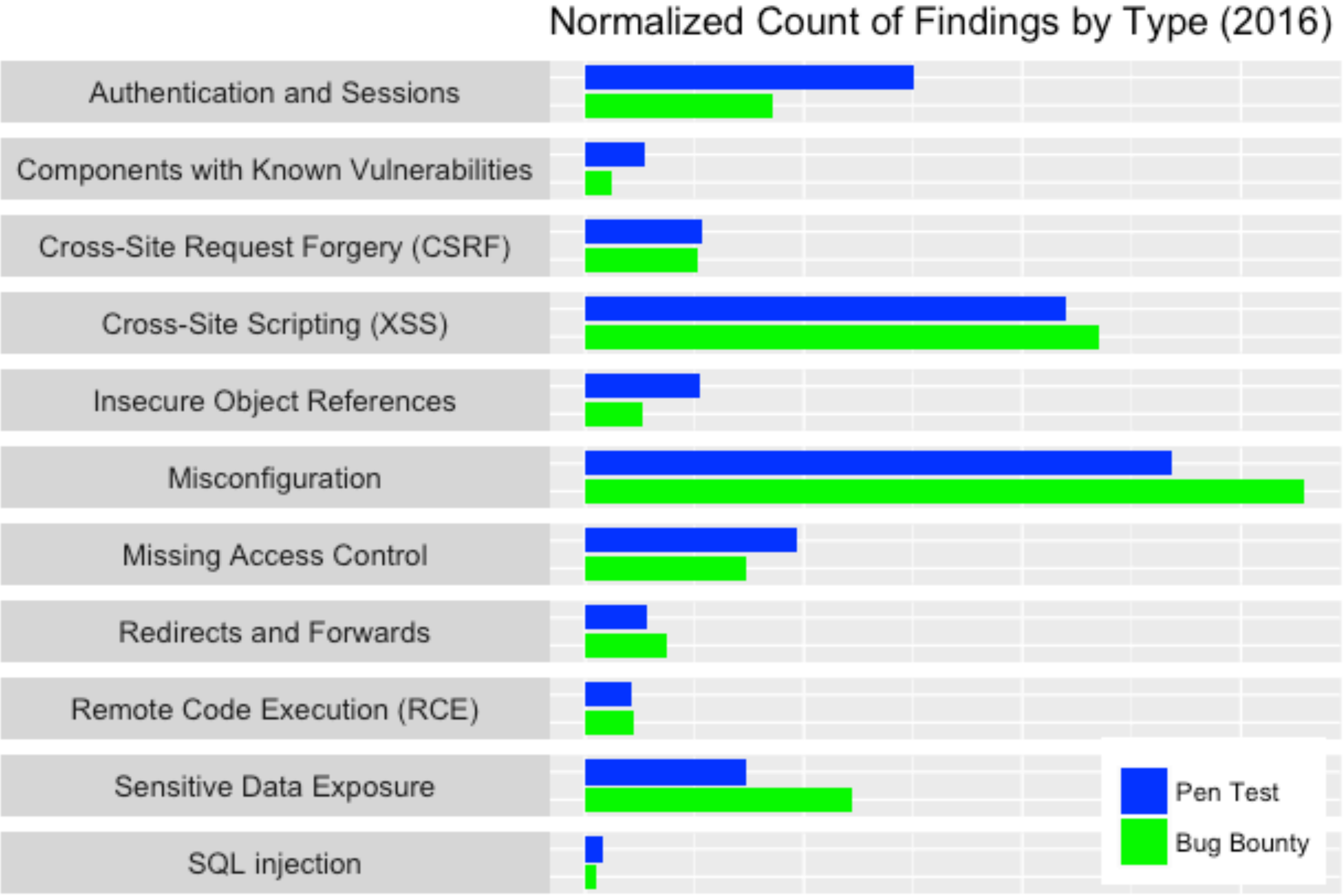
Acceptance State of Vulns Reported (2016)



~33%

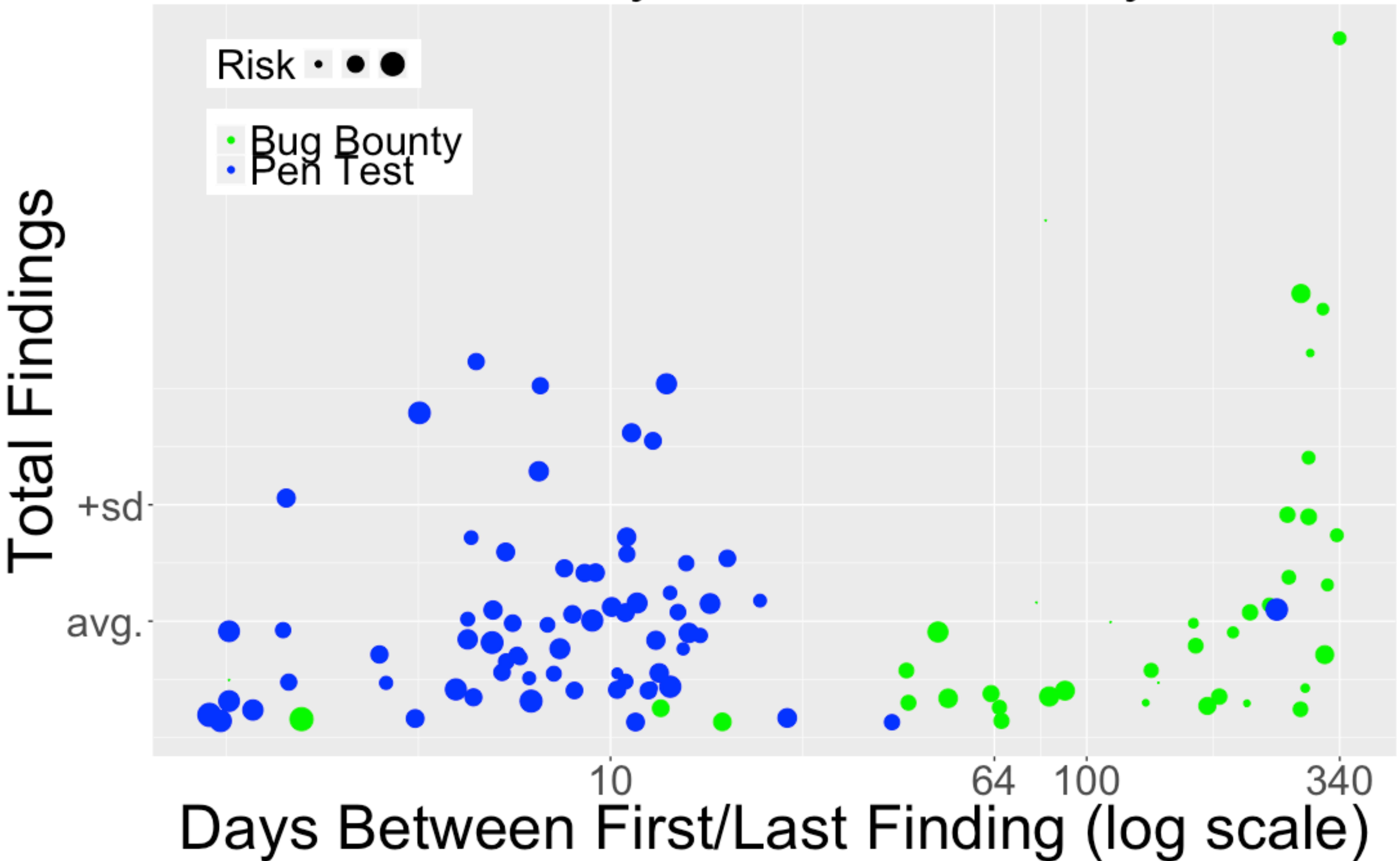
~87%

Noise increases cost of discovery and reduces efficiency.

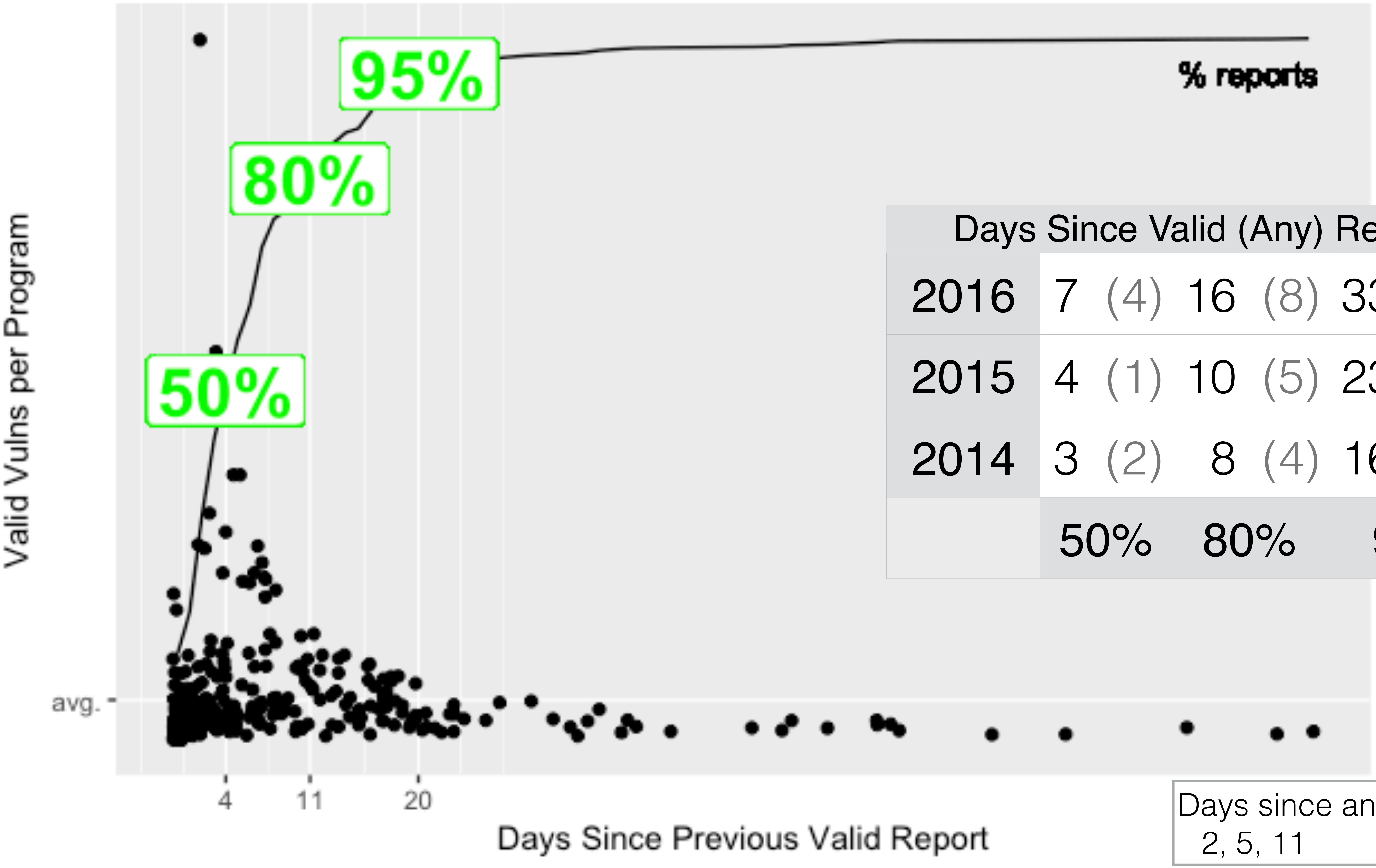


Normalized Count of Findings by Type (2016)

Efficiency of Risk Discovery



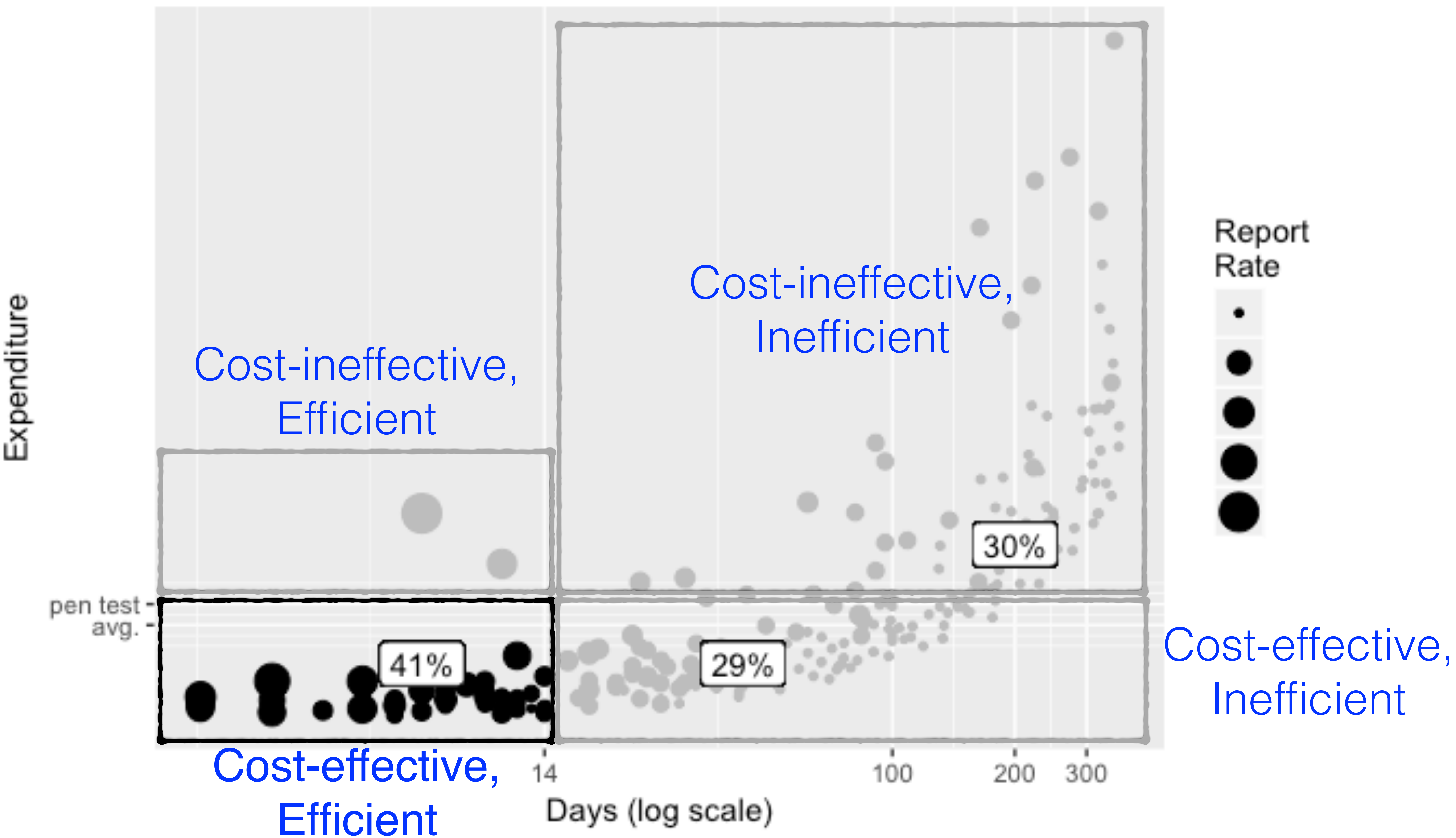
Exhausting the Pace of Vulns...or Attention?



Days Since Valid (Any) Report			
2016	7 (4)	16 (8)	33 (14)
2015	4 (1)	10 (5)	23 (11)
2014	3 (2)	8 (4)	16 (7)
	50%	80%	95%

Days since any report:
2, 5, 11

Risk Discovery Cost



Cost-ineffective, Efficient

Cost-ineffective, Inefficient

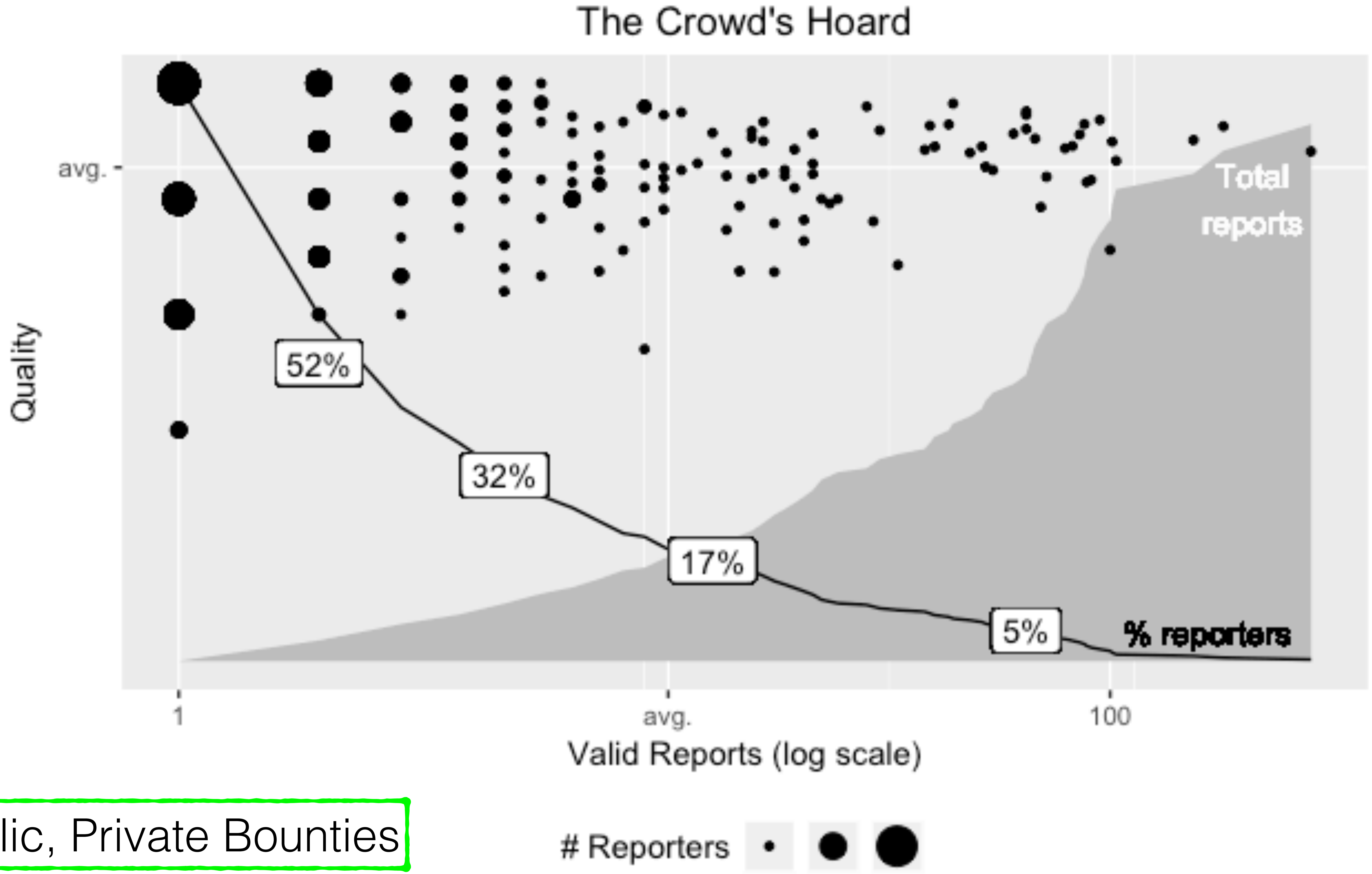
Cost-effective, Efficient

Cost-effective, Inefficient

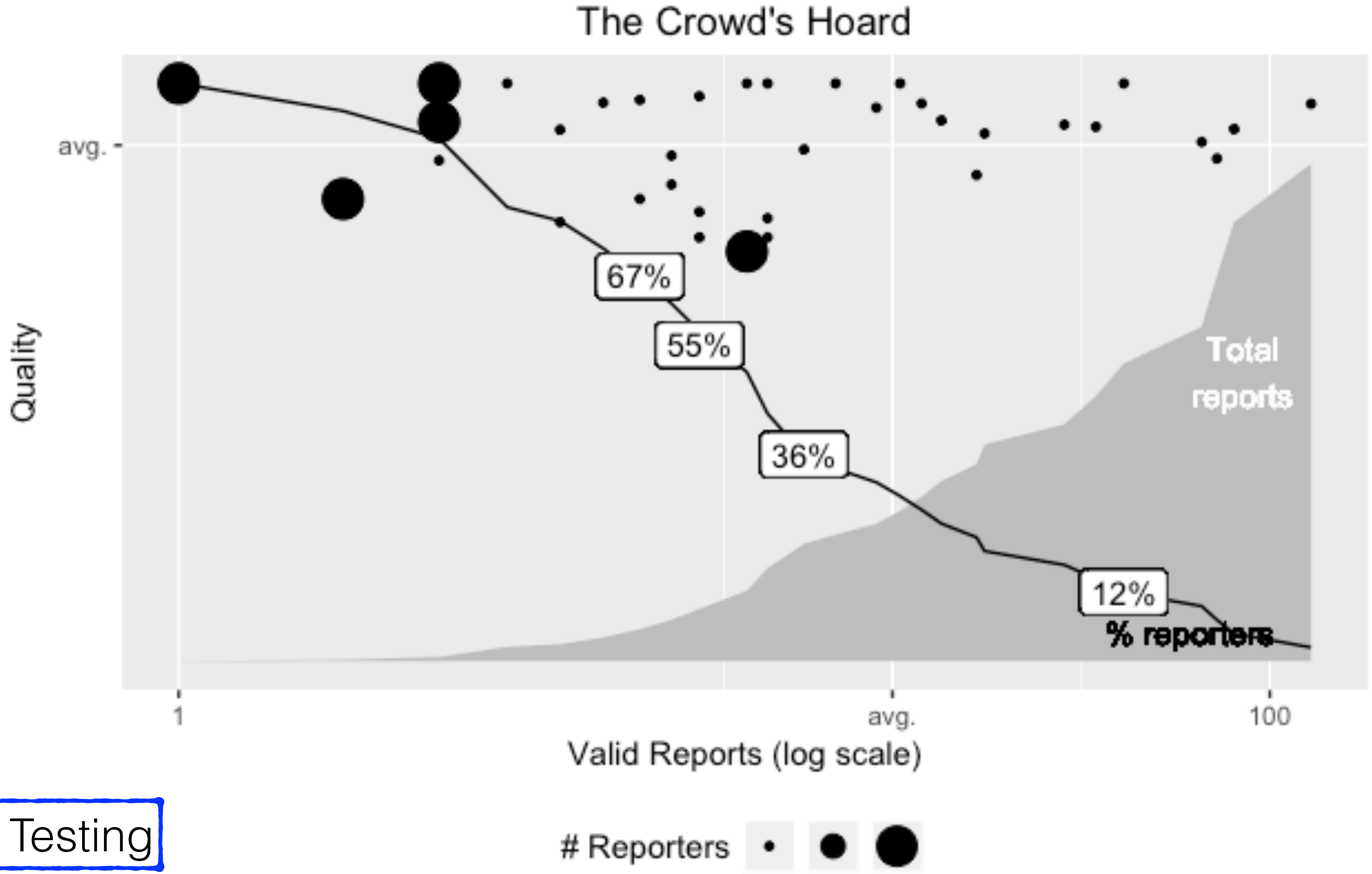
Where are the scanners?

Overlaps, gaps, and ceilings in capabilities.

Fixed-cost, typically efficient, but still requires triage and maintenance.



Public, Private Bounties


The Crowd's Hoard
Quality
avg.
67%
55%
36%
12%
Total reports
% reporters
1
avg.
100
Valid Reports (log scale)
# Reporters

Pen Testing

“We always have bugs.
Eyes are shallow.”

– Mike Shema’s Axiom of AppSec

BugOps vs. DevOps

Chasing bugs isn’t a strategy.

Risk reduction.

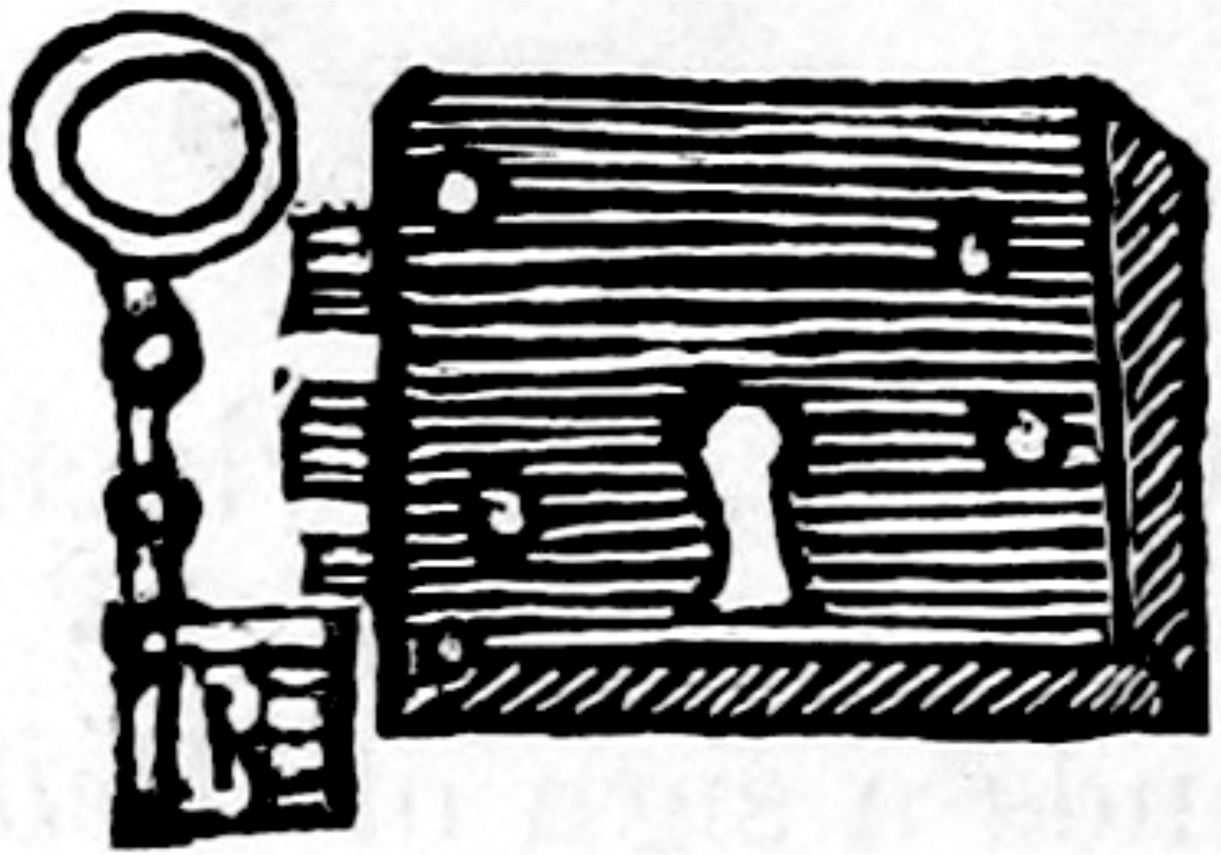
Advertiſement.

The Reader *is hereby advertiſed, that by reaſon of the preſent Contagion in* London, *which may unhappily cauſe an interruption aſwel of* Correſpondencies, *as of* Publick Meetings, *the printing of theſe* Philoſophical Tranſactions *may poſſibly for a while be intermitted; though endeavors ſhall be uſed to continue them, if it may be.*

"MS01-26, aka Double-Decode."

"MS01-33, c.f. Code Red."

"Trustworthy computing."

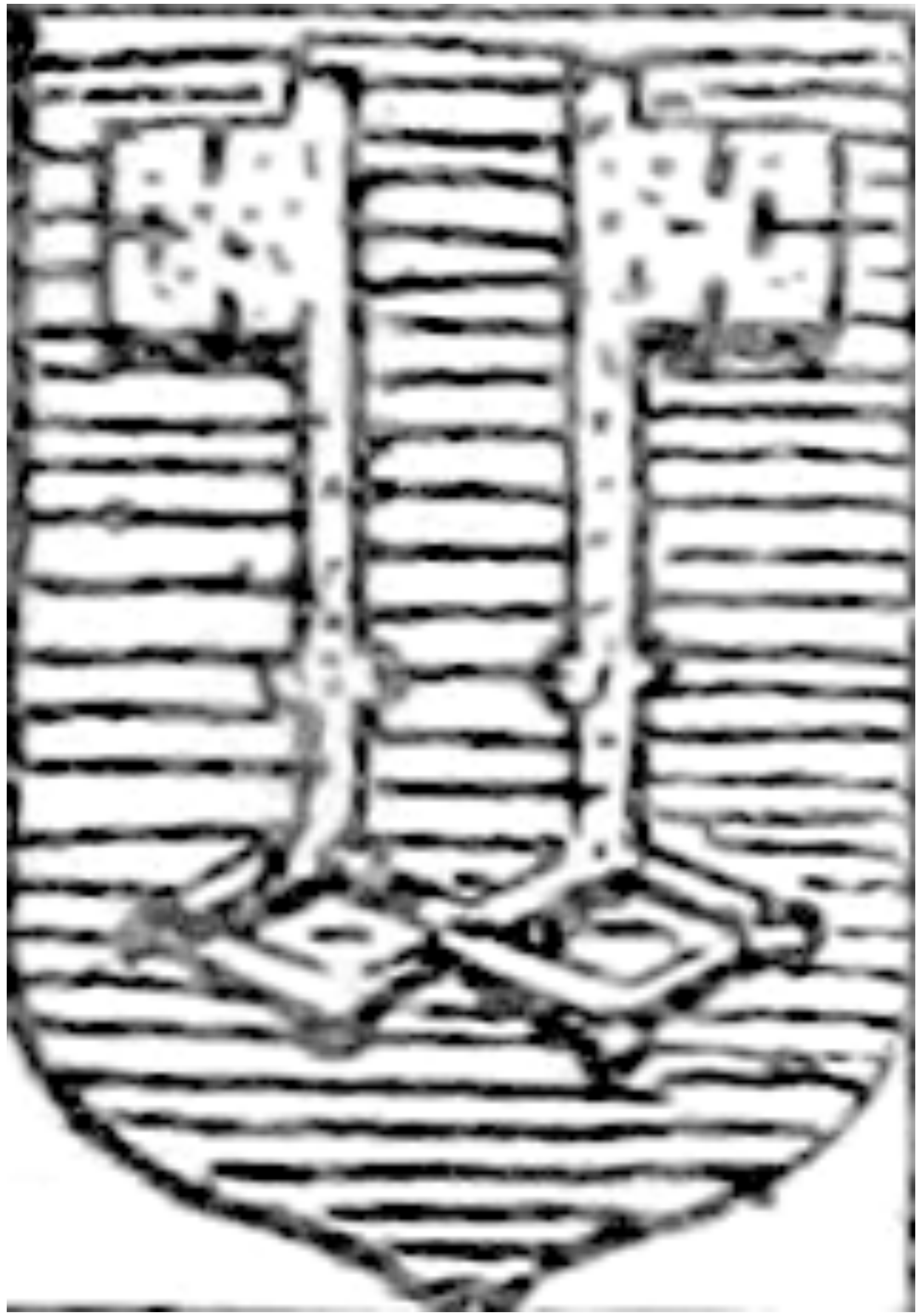


“OpenSSL 0.9.”

“OpenSSL 1.0.”

“LibreSSL, BoringSSL.”

“Remove code, re-architect API, revisit defaults.”

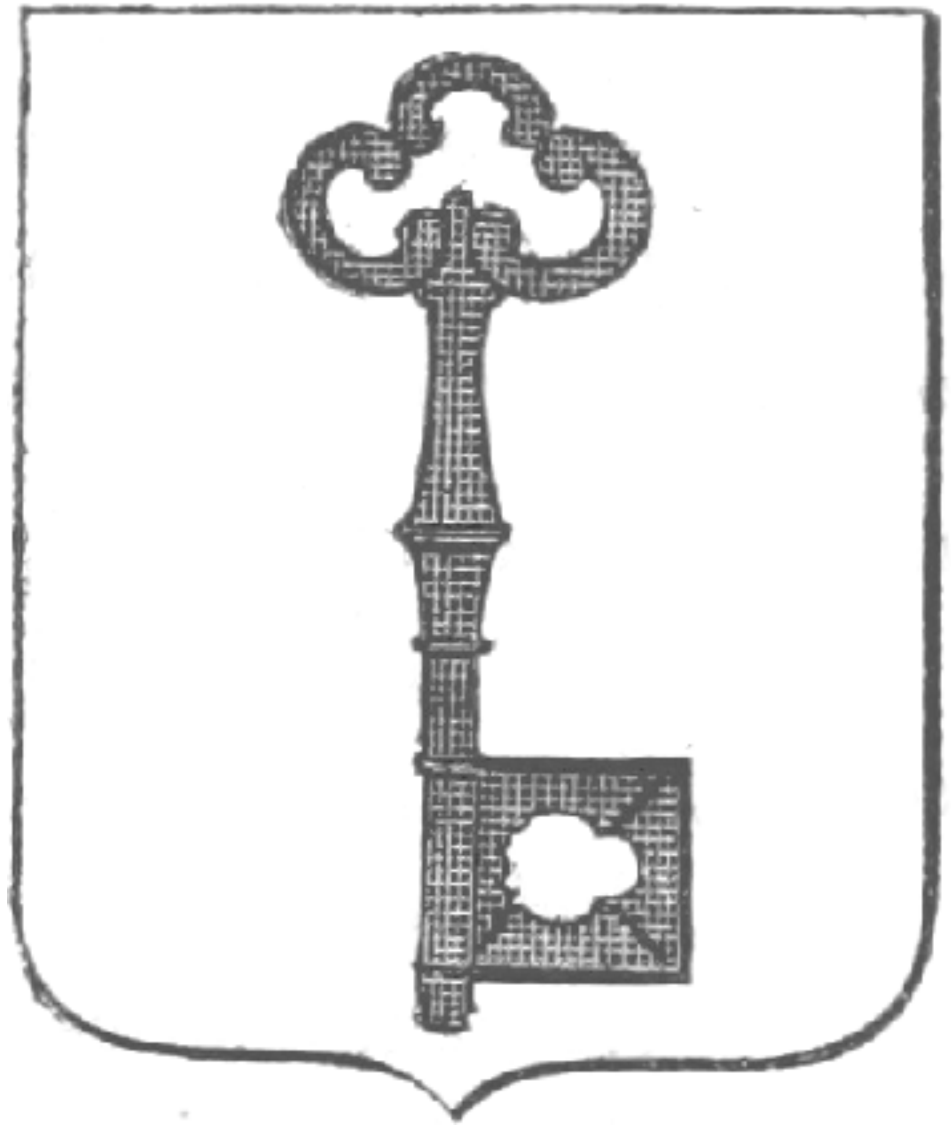


“You’re not using HTTPS.”

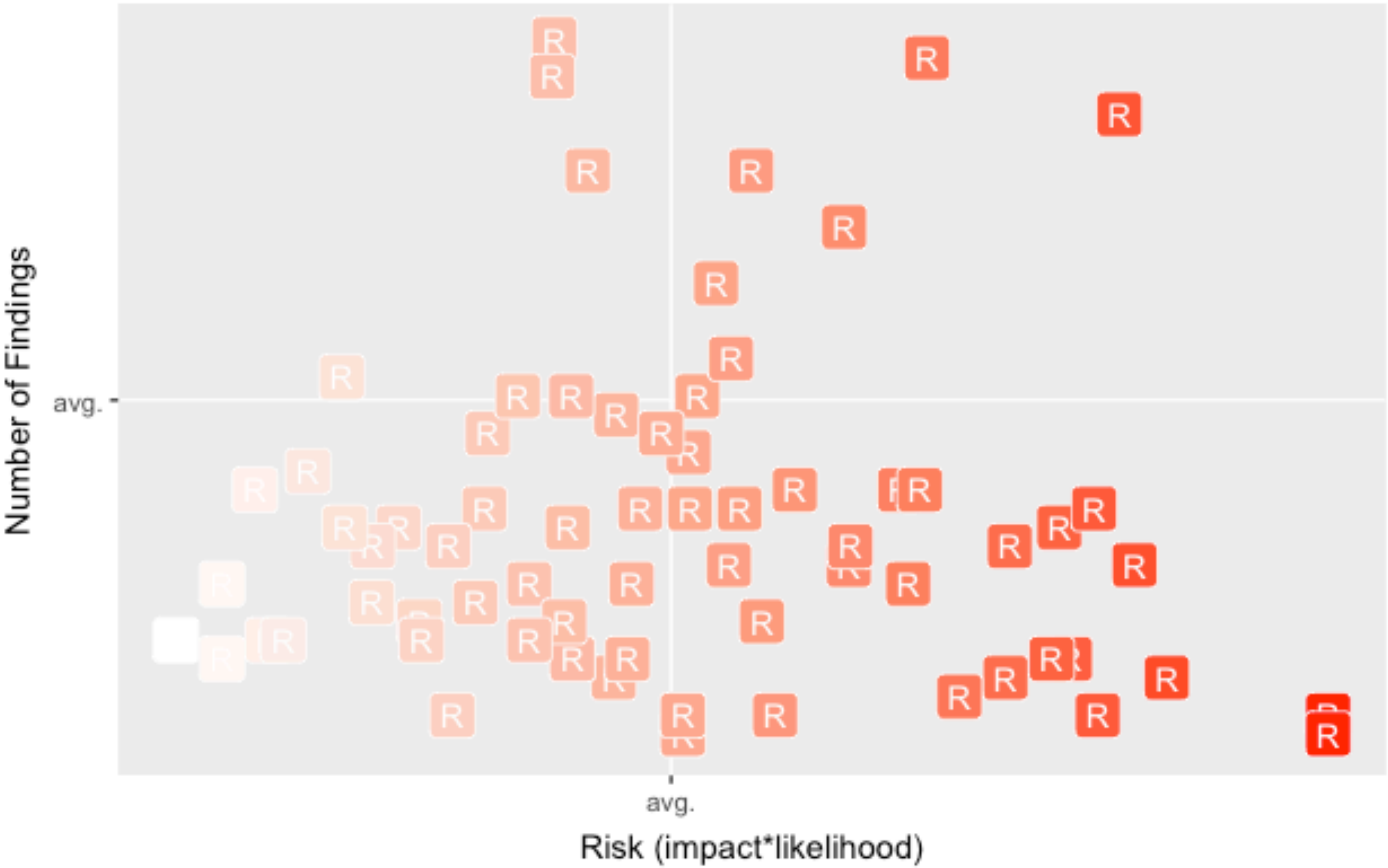
“Use HTTPS.”

“Seriously. Please use HTTPS.”

“Let’s Encrypt.”



Risk vs. Findings per Pen Test (2016)



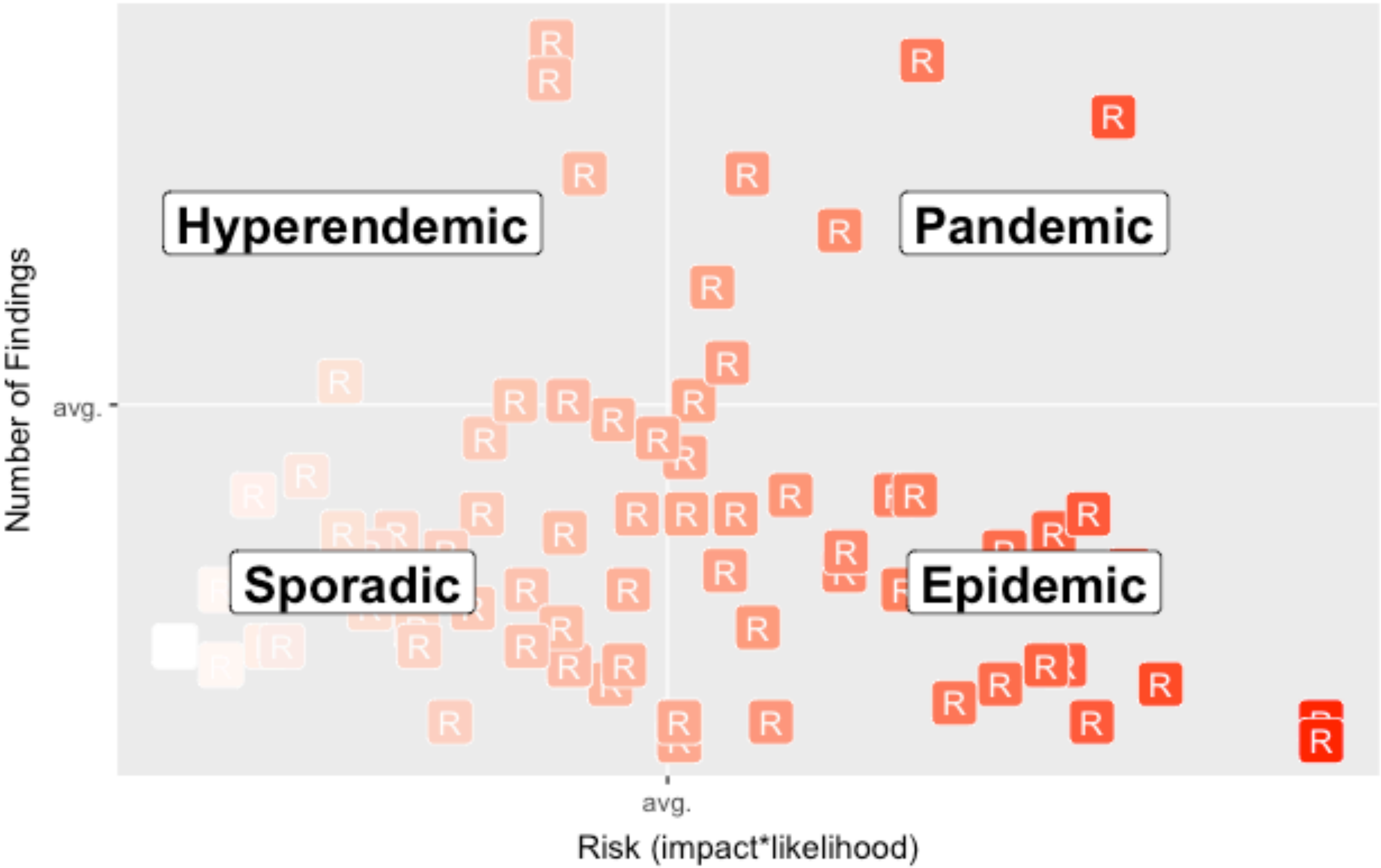
Risk Strategies

Decrease rate of reports for ___ vulns.

Increase speed of deploying fixes for ___ vulns.

Deploy ___ to counter ___ vuln class.

Endemic Risk Quadrants



Cacophony (Horde)

Users are stupid.

Devs are stupid.

Devs are lazy.

Always an easy fix.

Scrutiny (Crowd)

Safe defaults.

Share knowledge.

Lack of tools.

Complex systems.

Bounties

Formalizes coordinated disclosure process.

Learn against real-world apps.

Public bounty

Private bounty

Pen testing

Threat intel sharing

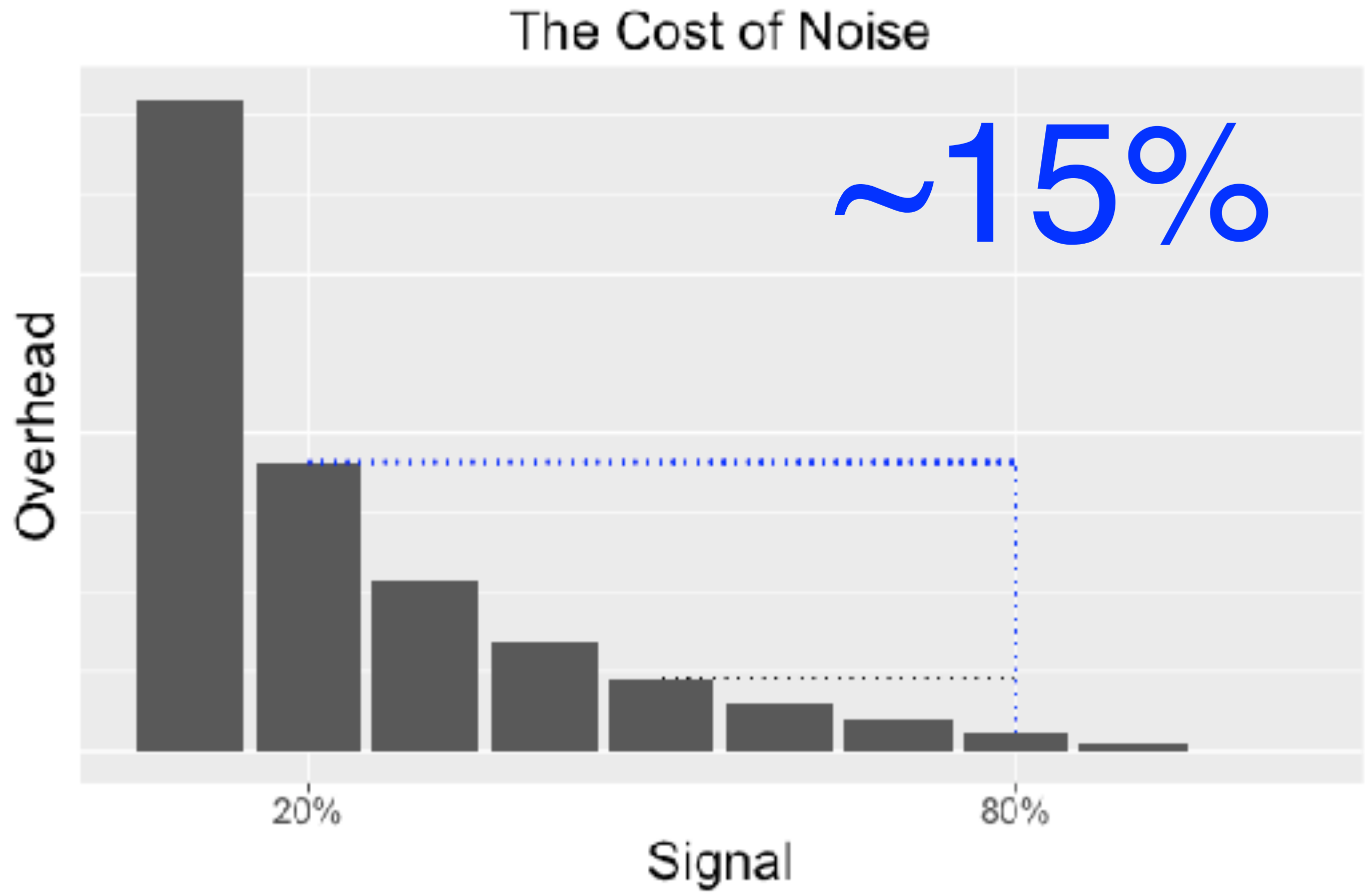
Fuzzing farms

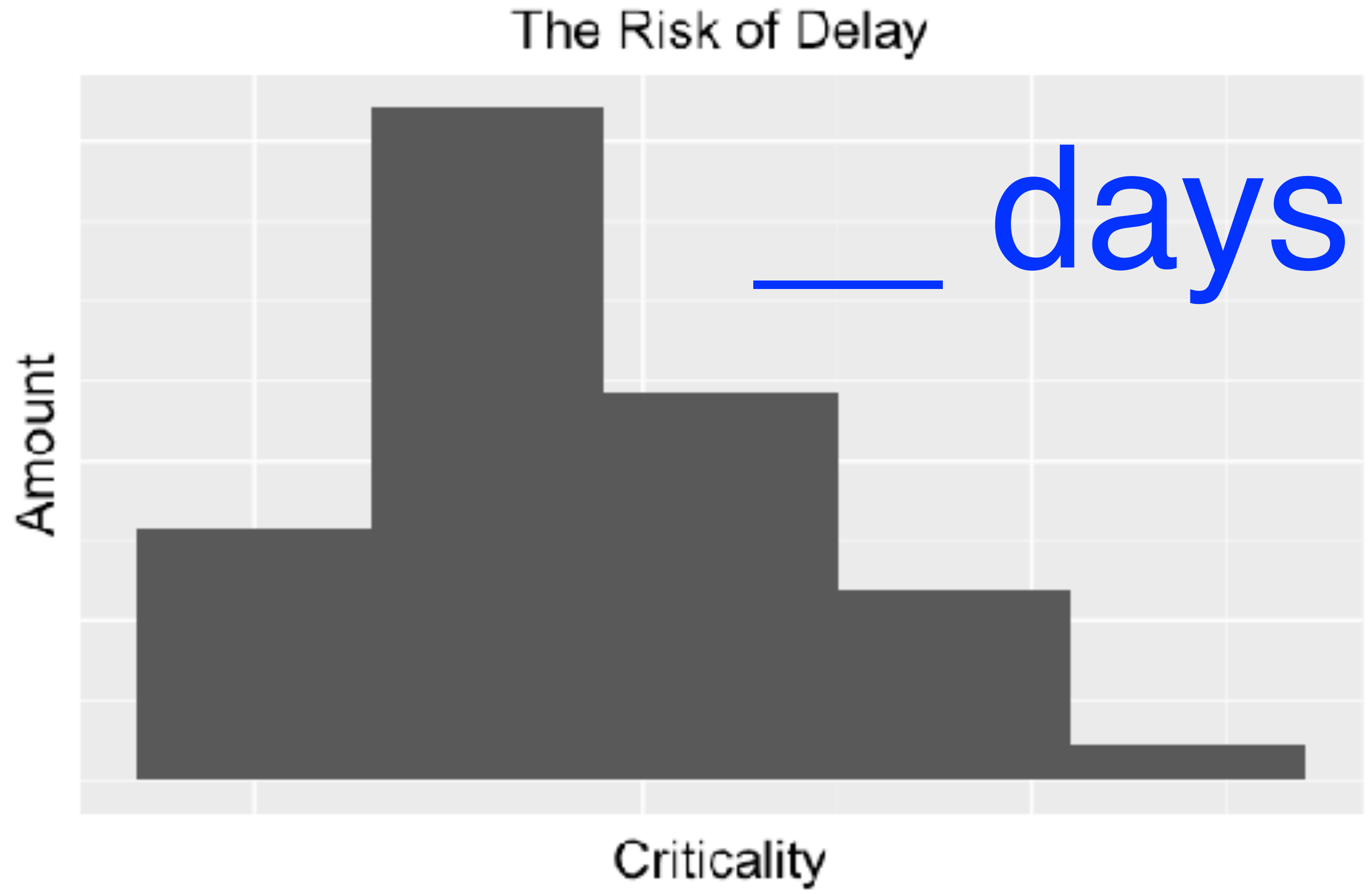
Crowds

Baseline —
Initial cost +
Ongoing maintenance

Vuln reports —
Reports/day,
Percent valid

Triage —
Reports/hour,
Hourly rate



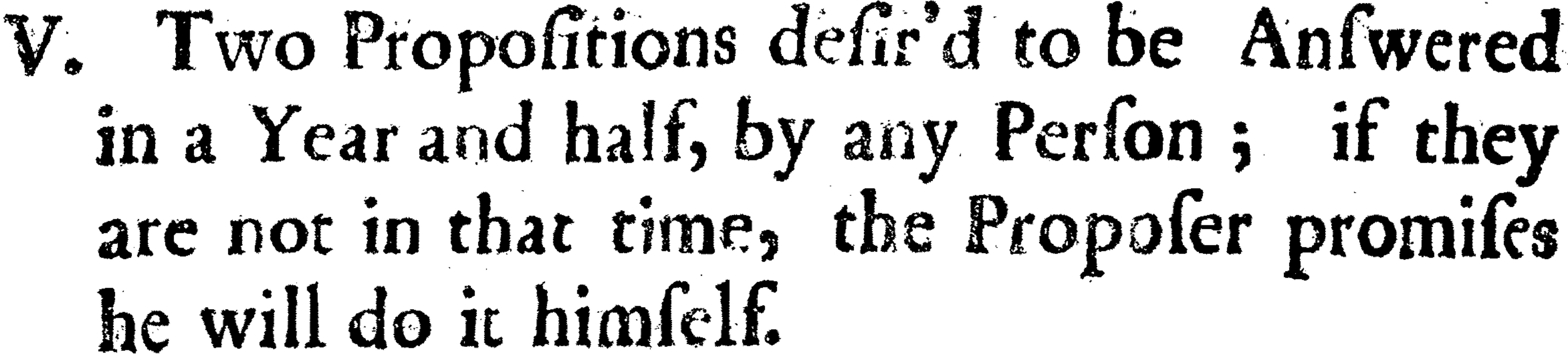


Find efficient vuln discovery methods, strive for automation.

Small crowds can have high impact.

Thank You!

blog.cobalt.io



V. Two Propoſitions deſir'd to be Anſwered in a Year and half, by any Perſon; if they are not in that time, the Propoſer promiſes he will do it himſelf.

Questions?

R — www.r-project.org

RStudio — www.rstudio.com

`data.table`

`ggplot`