Managing Crowdsourced Security

RVAsec
June 8, 2017

Mike Shema
mike@cobalt.io

“You see, in this world there’s two kinds of people, my friend: Those with loaded guns and those who dig. You dig.”

– Clint Eastwood, *The Good, the Bad, and the Ugly*.

“There are two kinds of spurs, my friend. Those that come in by the door; those that come in by the window.”

– Eli Wallach, *The Good, the Bad, and the Ugly*.

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.

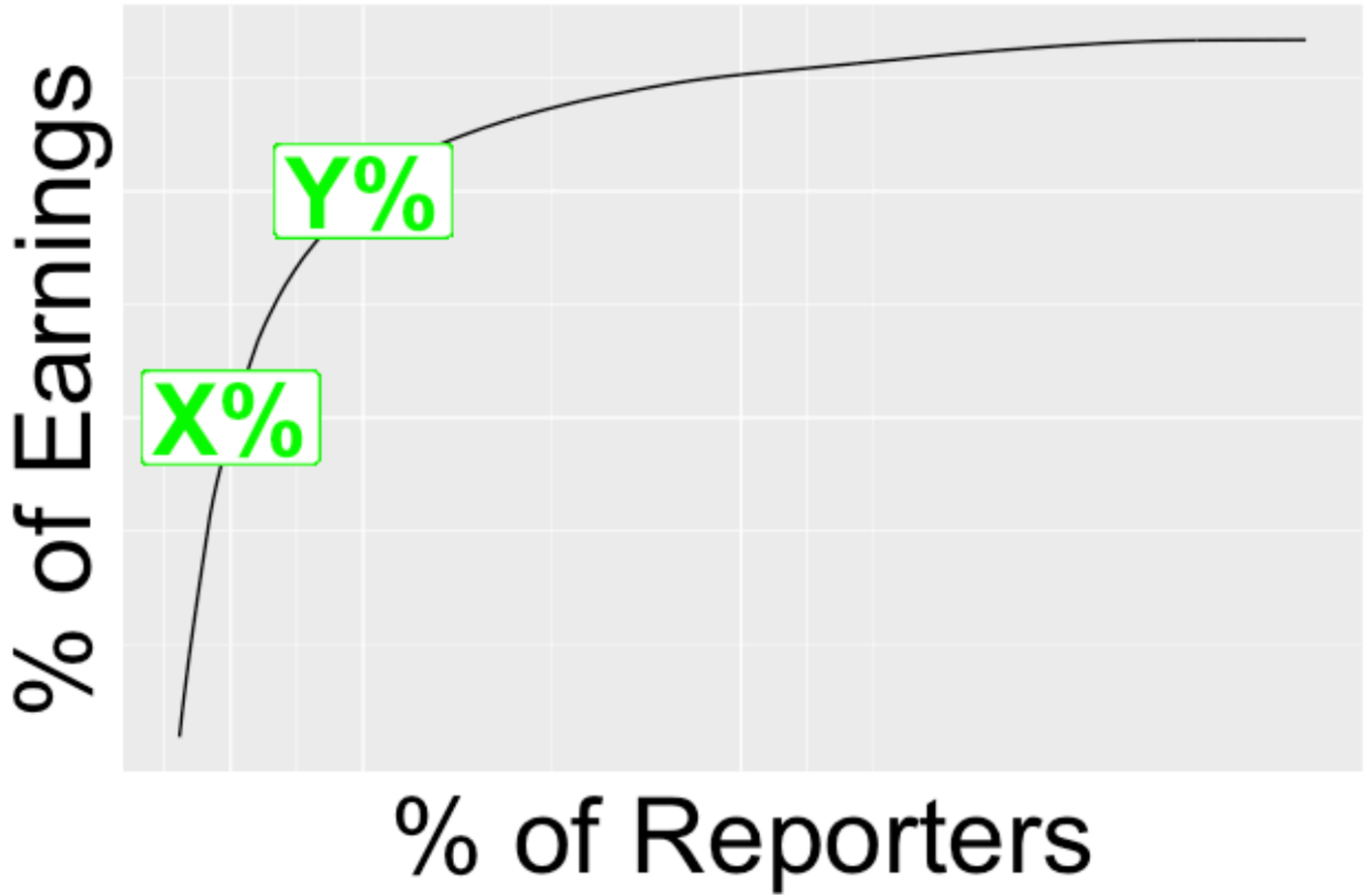
$50

Reflected XSS, self, no auth

$10,000

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

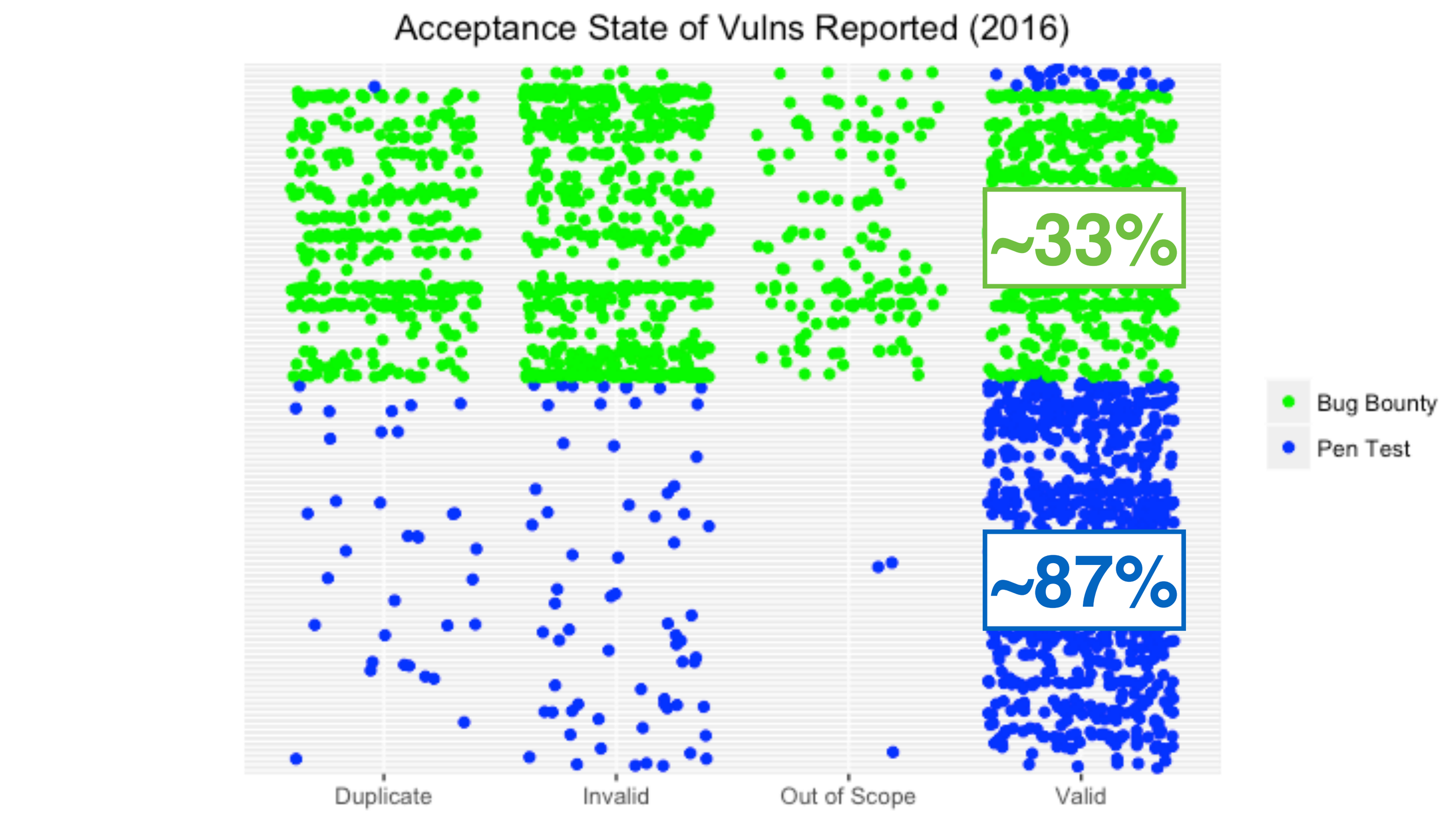
Bounties are an imperfect proxy for work, where earnings may diverge from effort.



100%

80%

50%


Acceptance State of Vulns Reported (2016)
~33%
~87%
Bug Bounty
Pen Test
Duplicate
Invalid
Out of Scope
Valid

Noise increases cost of discovery and reduces efficiency.

Filters

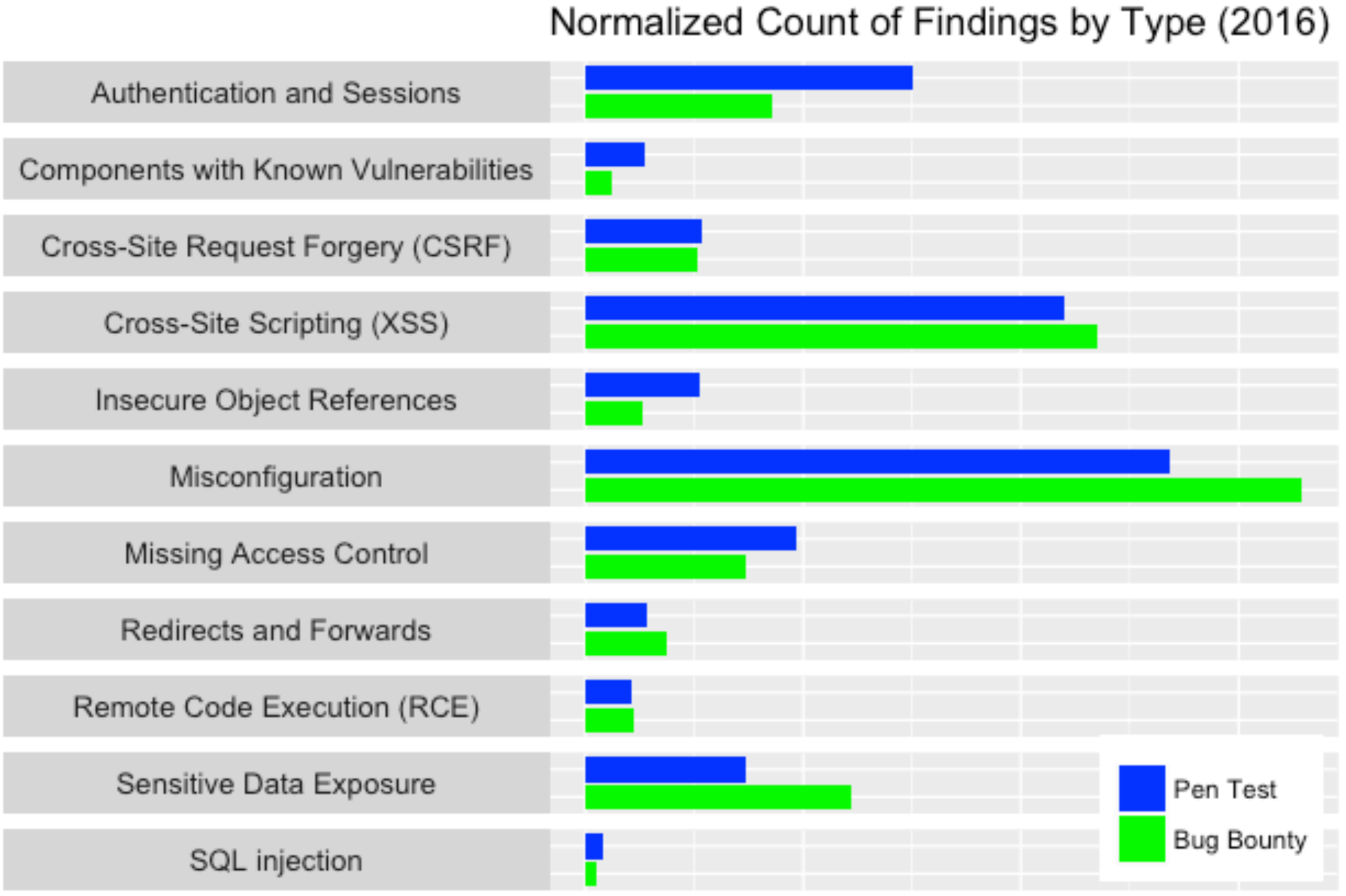
Clear, concise documentation

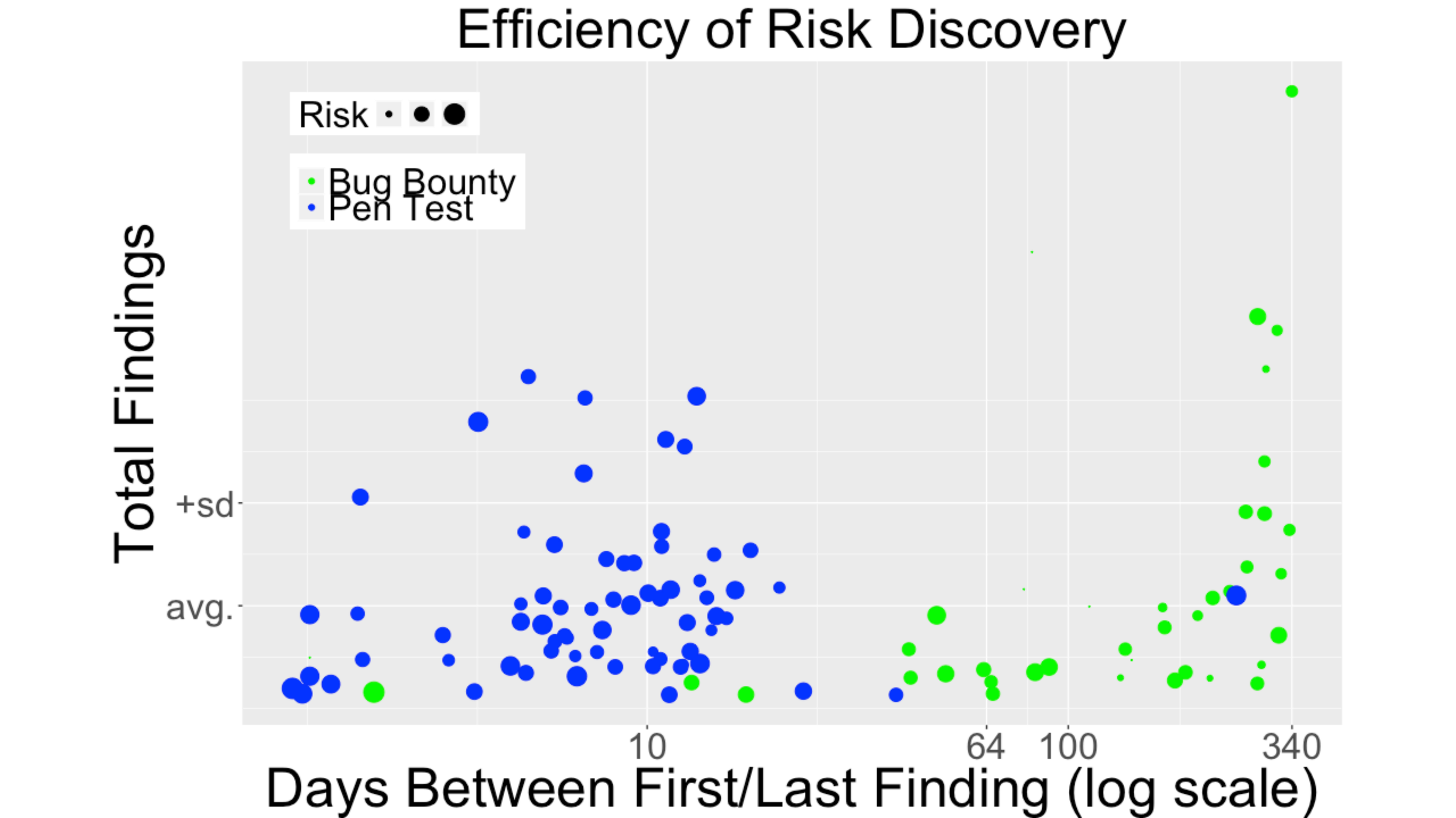
Scope

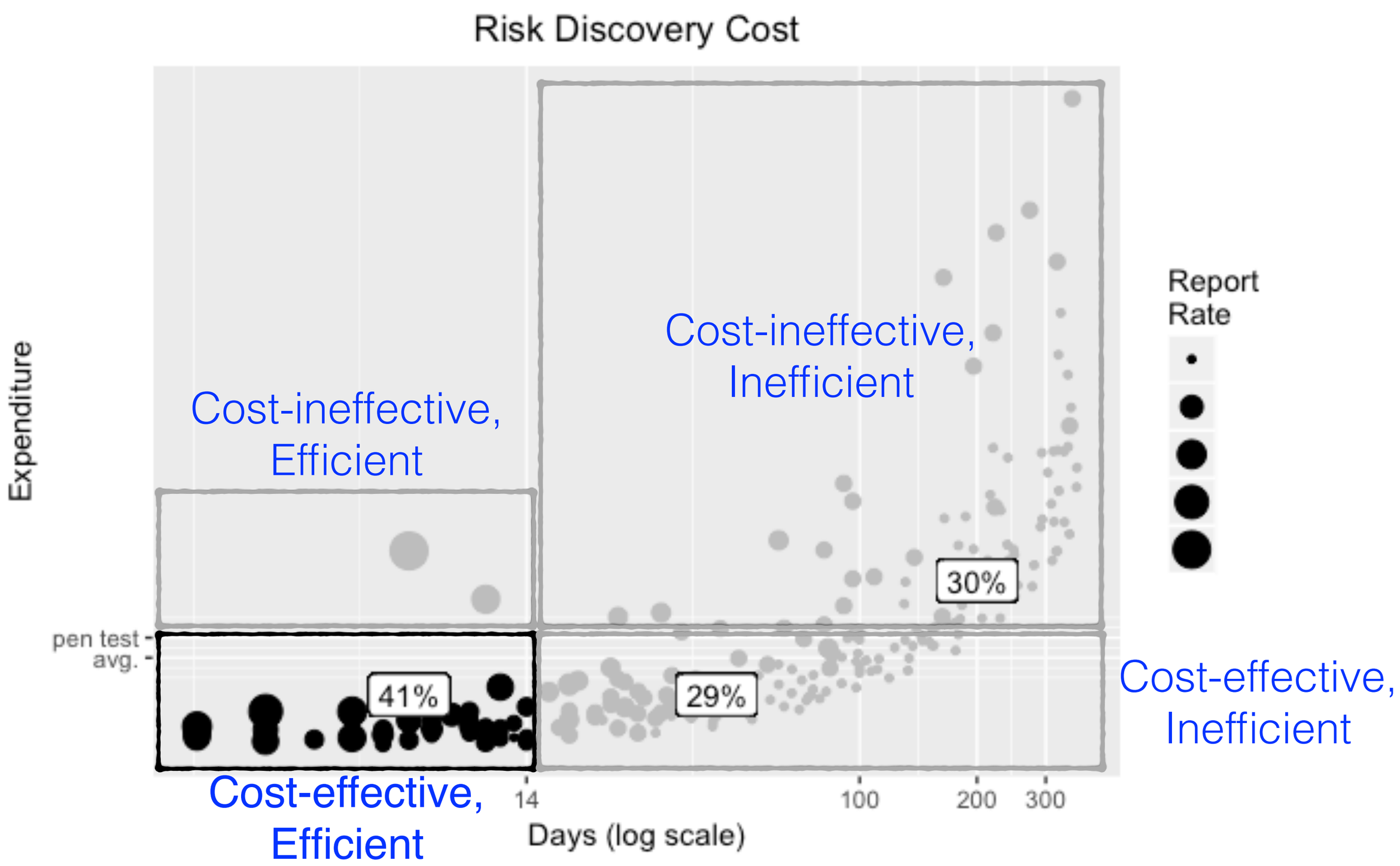
Rules of engagement

Practical SLAs for responses

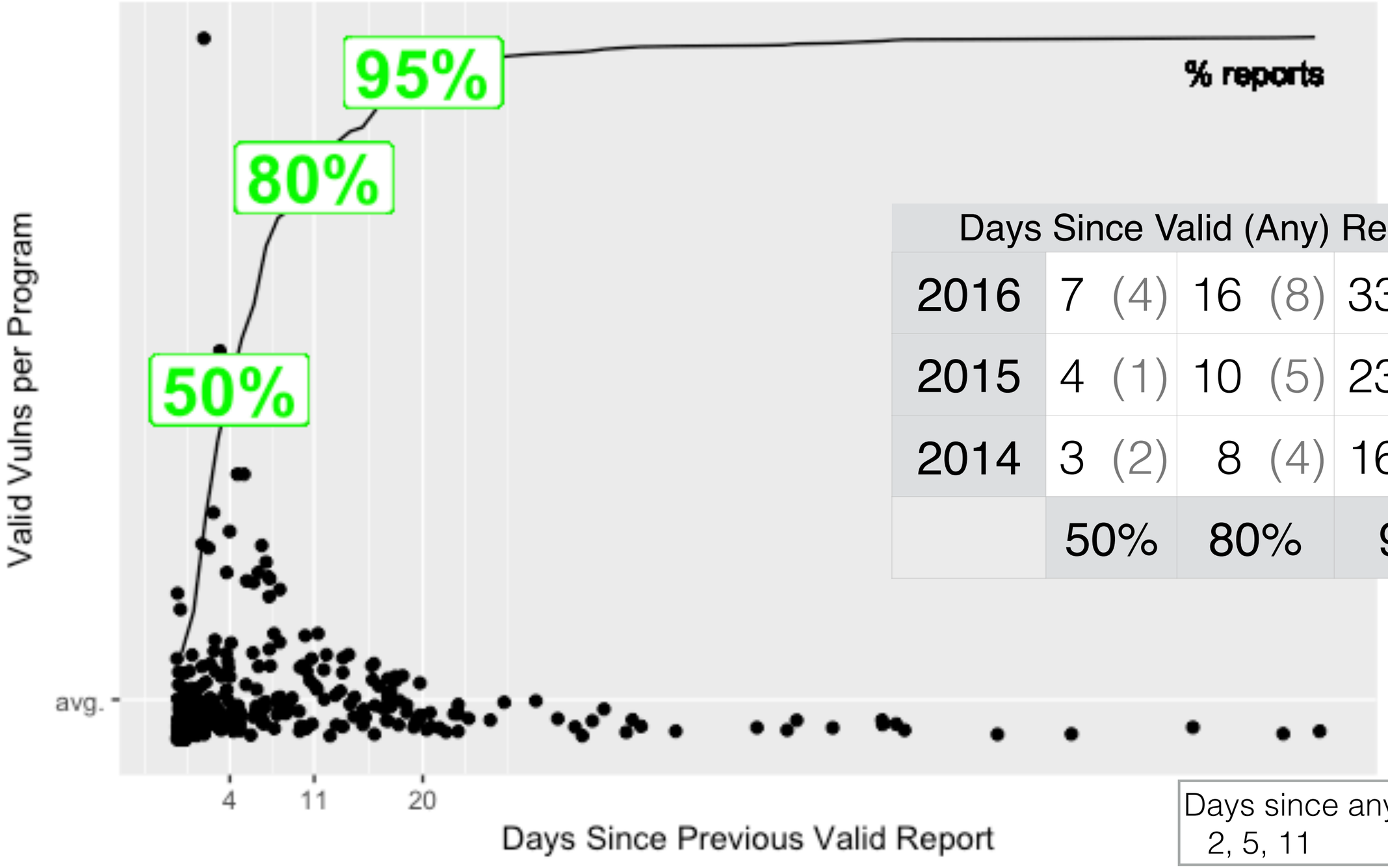
Expectations of reasonable threat models


Normalized Count of Findings by Type (2016)
Authentication and Sessions
Components with Known Vulnerabilities
Cross-Site Request Forgery (CSRF)
Cross-Site Scripting (XSS)
Insecure Object References
Misconfiguration
Missing Access Control
Redirects and Forwards
Remote Code Execution (RCE)
Sensitive Data Exposure
SQL injection
Pen Test
Bug Bounty


Efficiency of Risk Discovery
Risk
Bug Bounty
Pen Test
Total Findings
+sd
avg.
10
64
100
340
Days Between First/Last Finding (log scale)


Risk Discovery Cost
Expenditure
pen test avg.
Cost-ineffective, Efficient
Cost-ineffective, Inefficient
Cost-effective, Efficient
Cost-effective, Inefficient
41%
29%
30%
14
100
200
300
Days (log scale)
Report Rate

Exhausting the Pace of Vulns...or Attention?



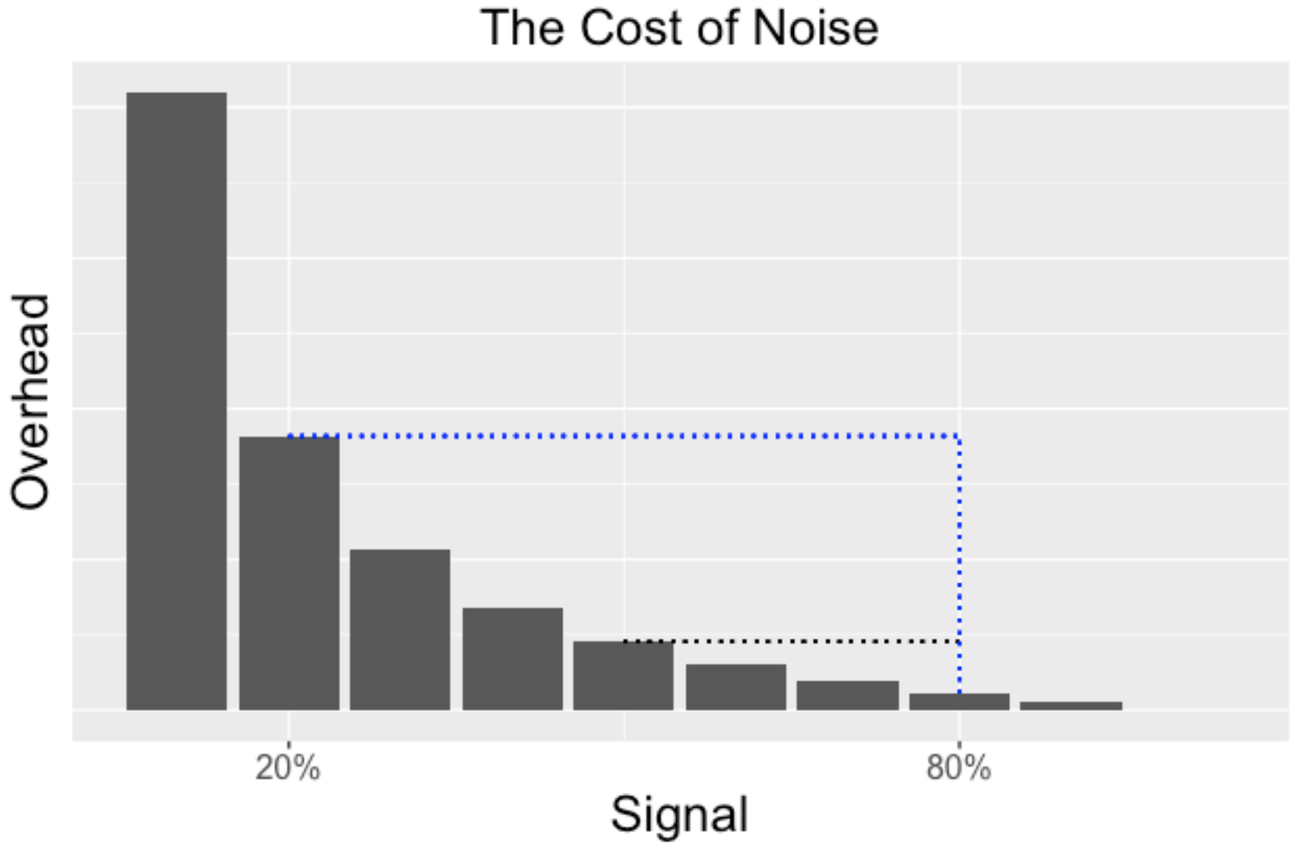
Days Since Valid (Any) Report			
2016	7 (4)	16 (8)	33 (14)
2015	4 (1)	10 (5)	23 (11)
2014	3 (2)	8 (4)	16 (7)
	50%	80%	95%

Days since any report:
2, 5, 11

Baseline —
  Initial cost +
  Ongoing maintenance

Volume —
  Reports/day,
  Percent valid

Triage —
  Reports/hour,
  Hourly rate

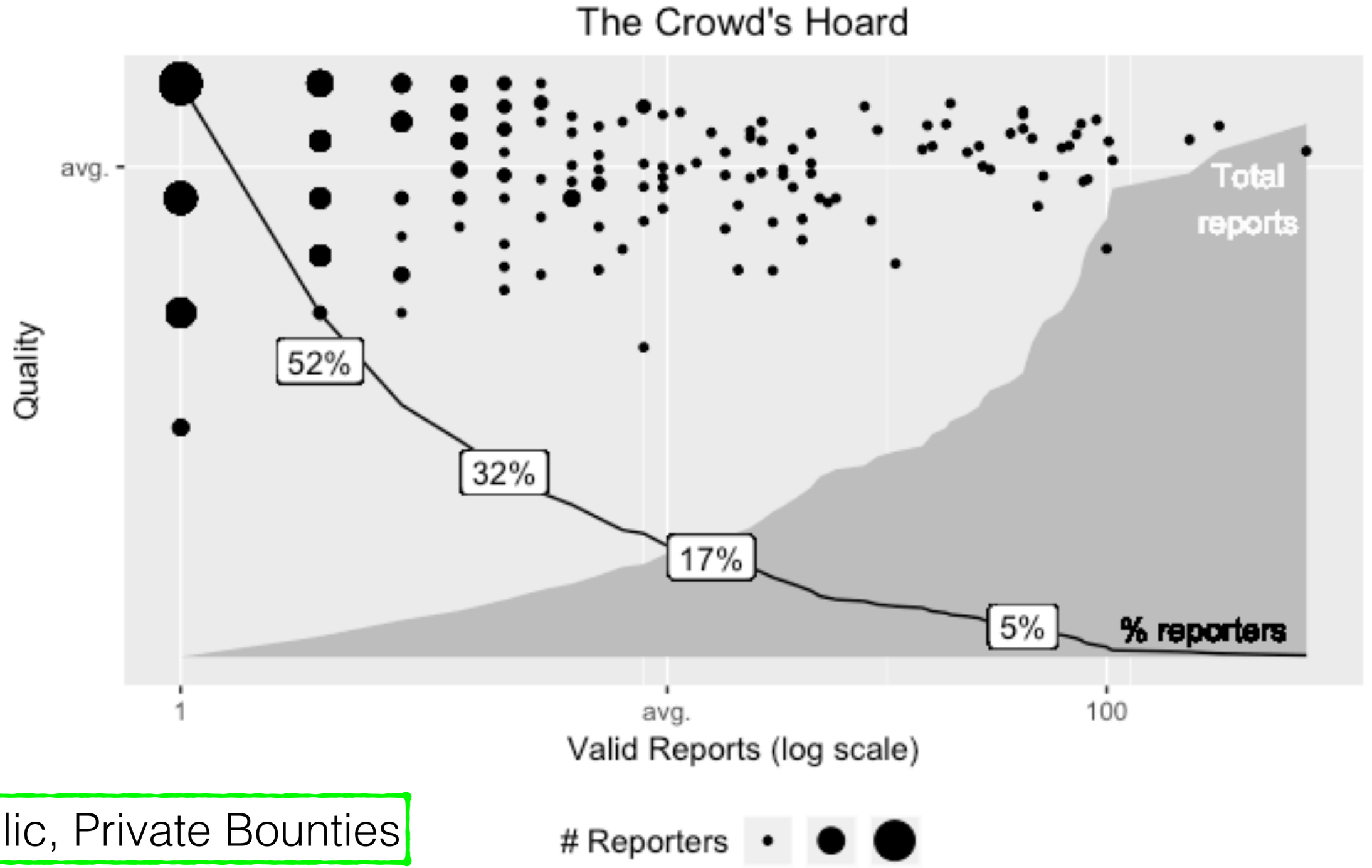


~15% savings

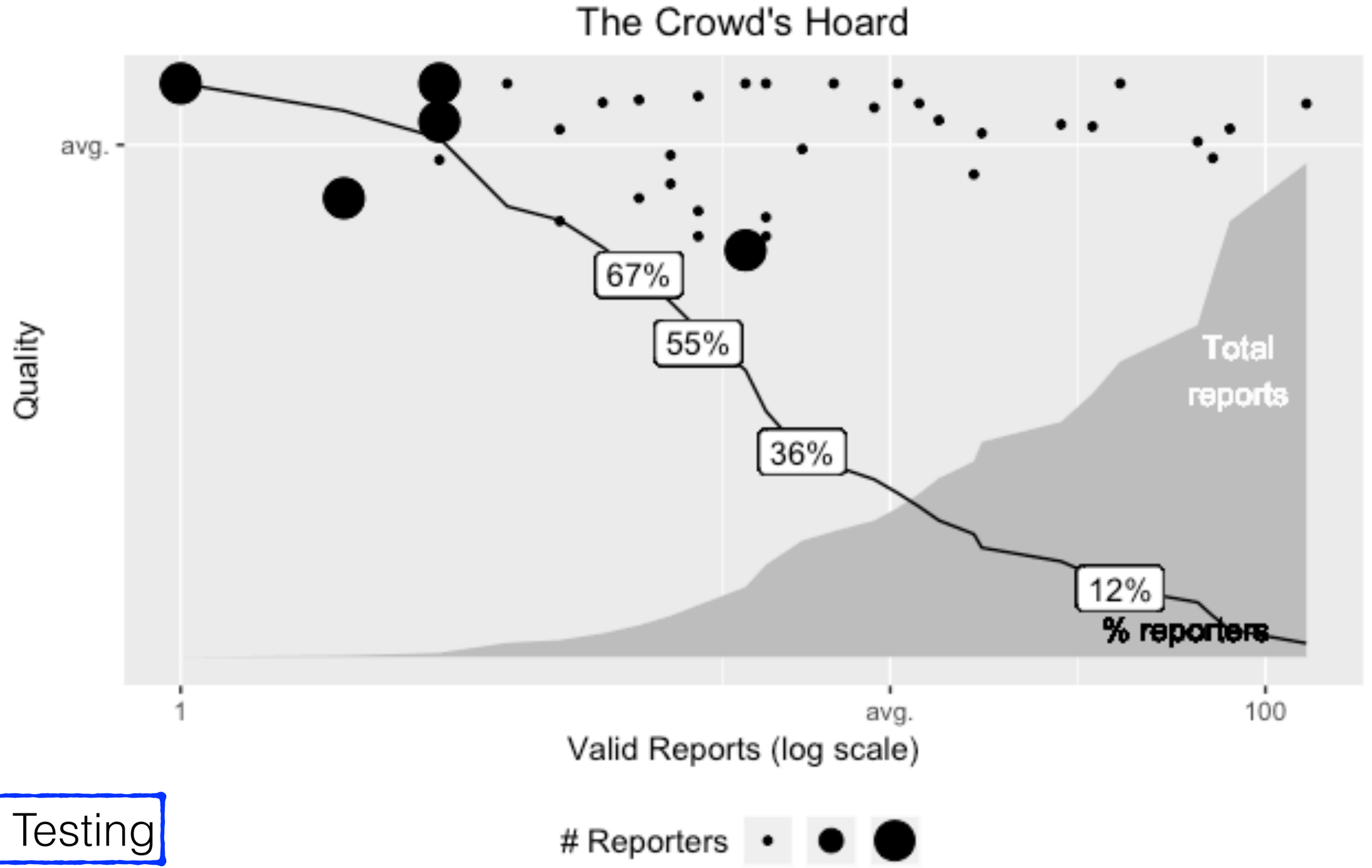
Where are the scanners?

Overlaps, gaps, and ceilings in capabilities.

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



Public, Private Bounties


The Crowd's Hoard
avg.
Quality
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.

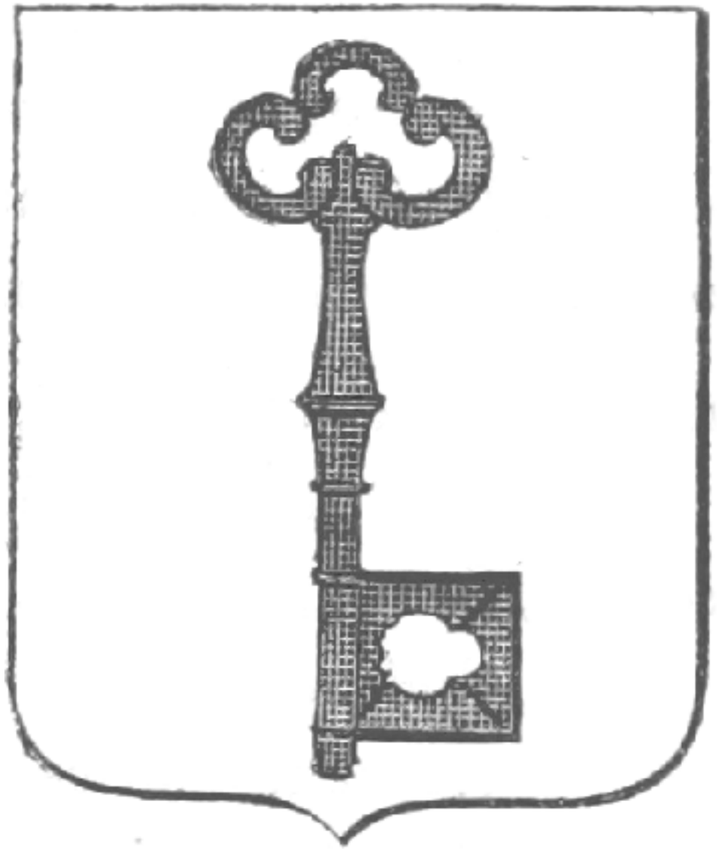
Risk reduction.

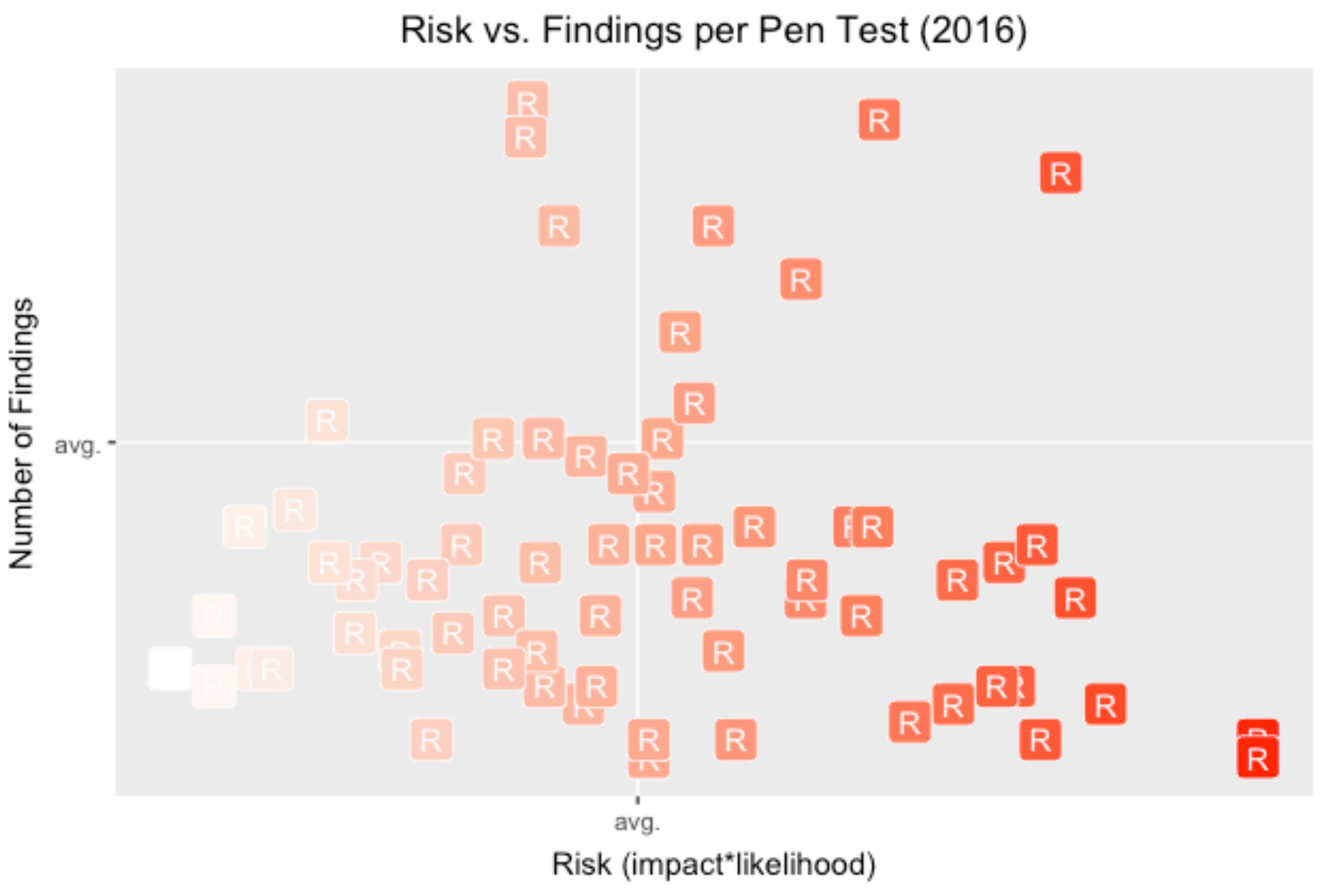
“You’re not using HTTPS.”

“Use HTTPS.”

“Seriously. Please use HTTPS.”

“Let’s Encrypt.”



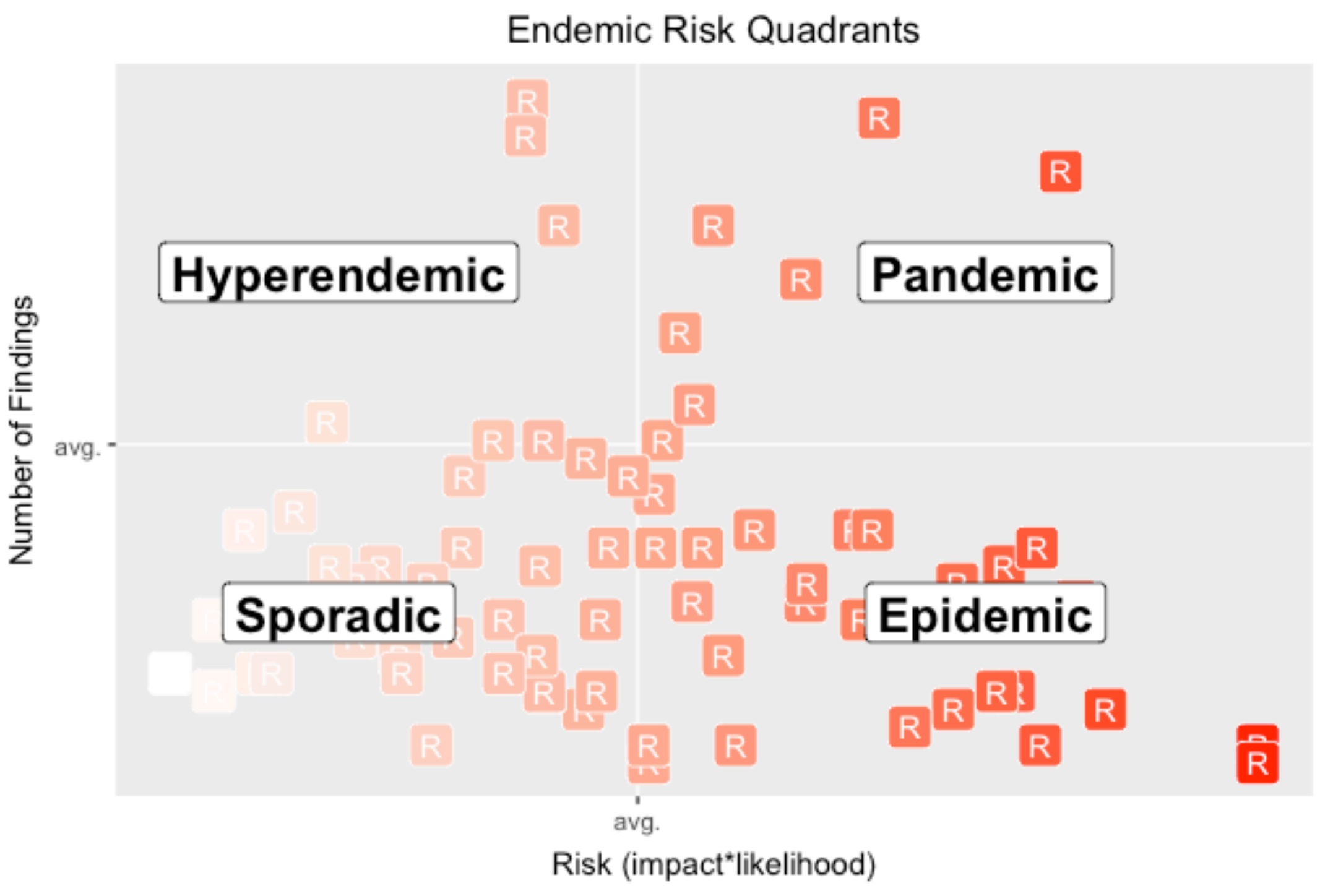

Risk vs. Findings per Pen Test (2016)
Number of Findings
avg.
avg.
Risk (impact*likelihood)

Risk Strategies

Decrease rate of reports for ___ vulns.

Increase speed of deploying fixes for ___ vulns.

Deploy ___ to counter ___ vuln class.


Endemic Risk Quadrants
Hyperendemic
Pandemic
Sporadic
Epidemic
Number of Findings
avg.
avg.
Risk (impact*likelihood)

Realistic threat models.

Incentives oriented towards quality and effort.

Machine-readable reports.

Bounties

Public bounty

Private bounty

Pen testing

Threat intel sharing

Fuzzing farms

Crowds

Find efficient vuln discovery methods, strive for automation.

Small crowds can have high impact.

Thank You!

blog.cobalt.io

Questions?

R —
www.r-project.org

RStudio —
www.rstudio.com

`data.table`

`ggplot`