Crowdsourced Security — The Good, the Bad, & the Ugly

(ISC)^2 Security Congress
September 25, 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.”

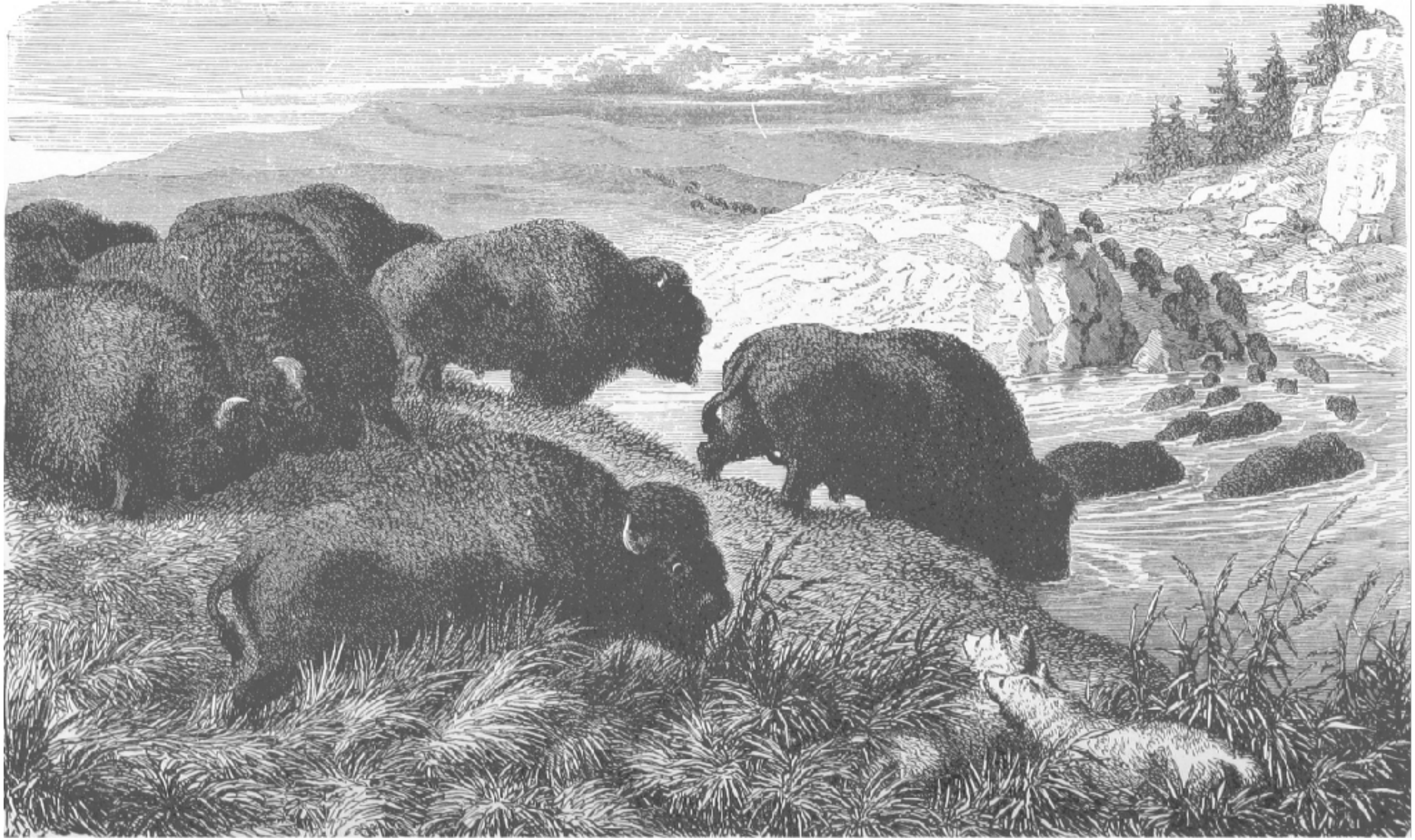
– Eli Wallach, *The Good, the Bad, and the Ugly*.

Uneasy Alliances

“What’s the price for this vuln?”
— Bounties

“What’s the cost to fix this vuln?”
— DevOps

“What’s the value of (& budget for) finding vulns?”
— CSOs



Disclosure Happens

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

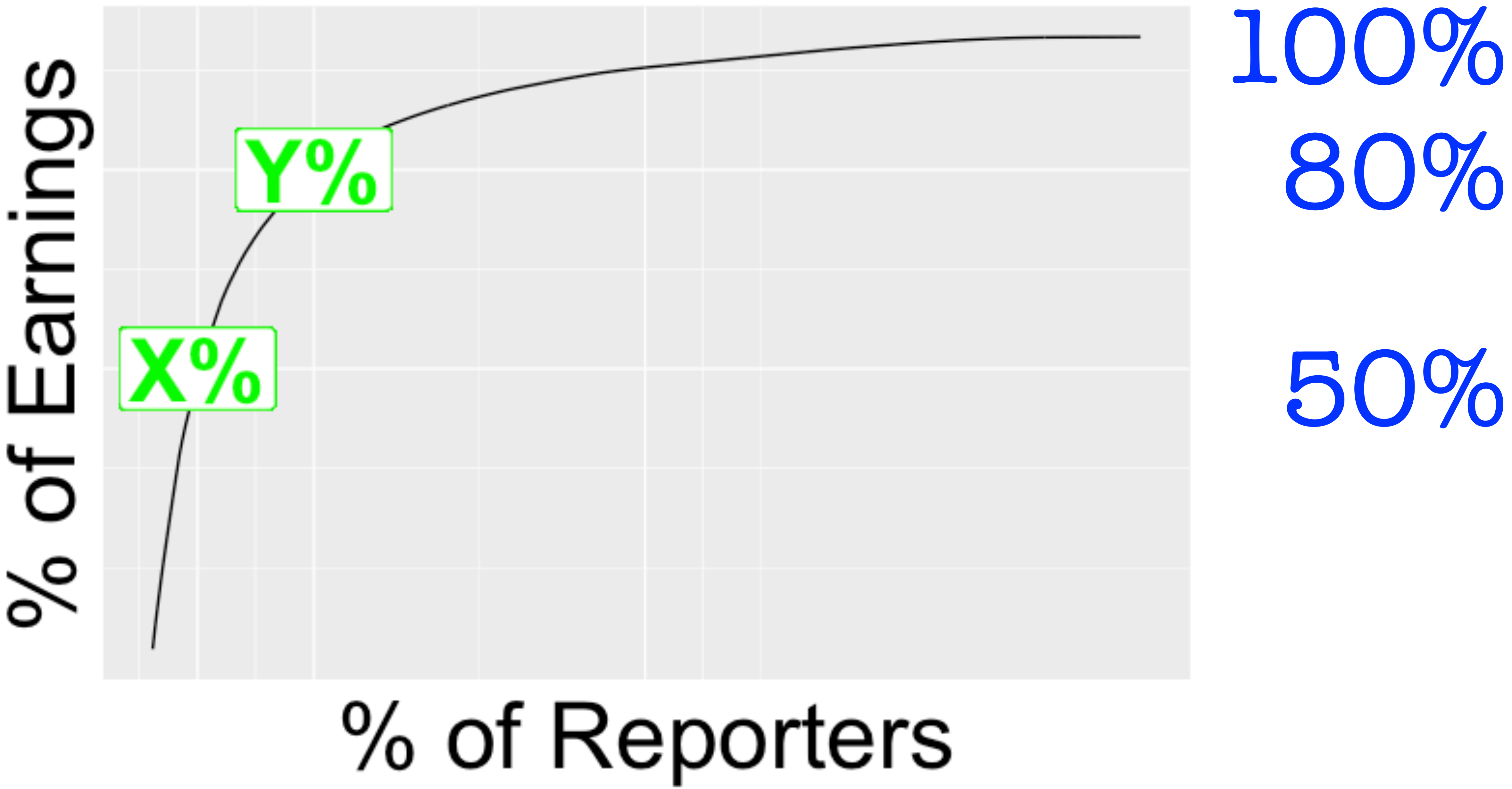
$0 — $15K

~$800 avg.

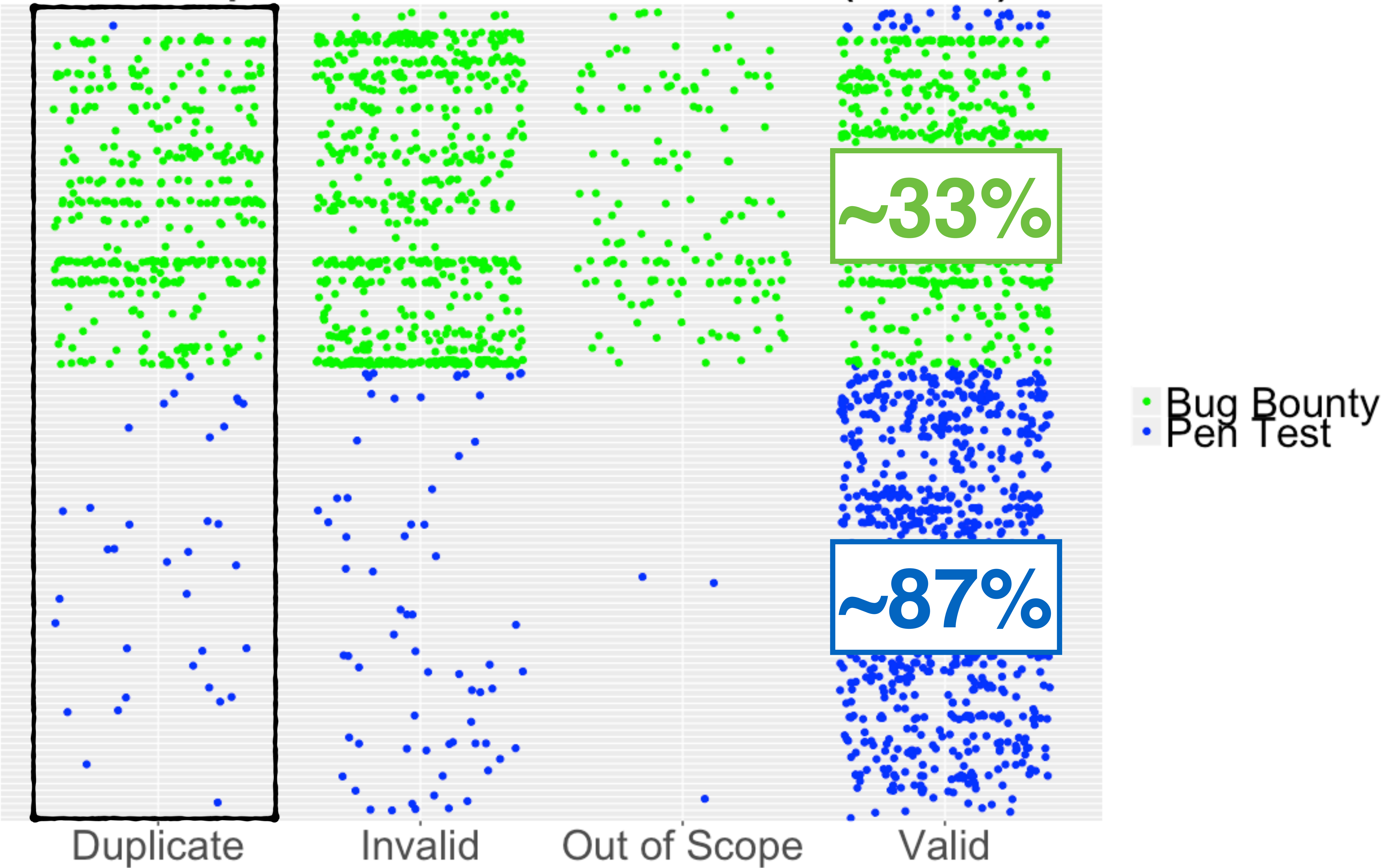
$50
Reflected XSS, self,
no auth

$10,000
XSS any auth’d user,
access sensitive info

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



Acceptance State of Vulns (2016)

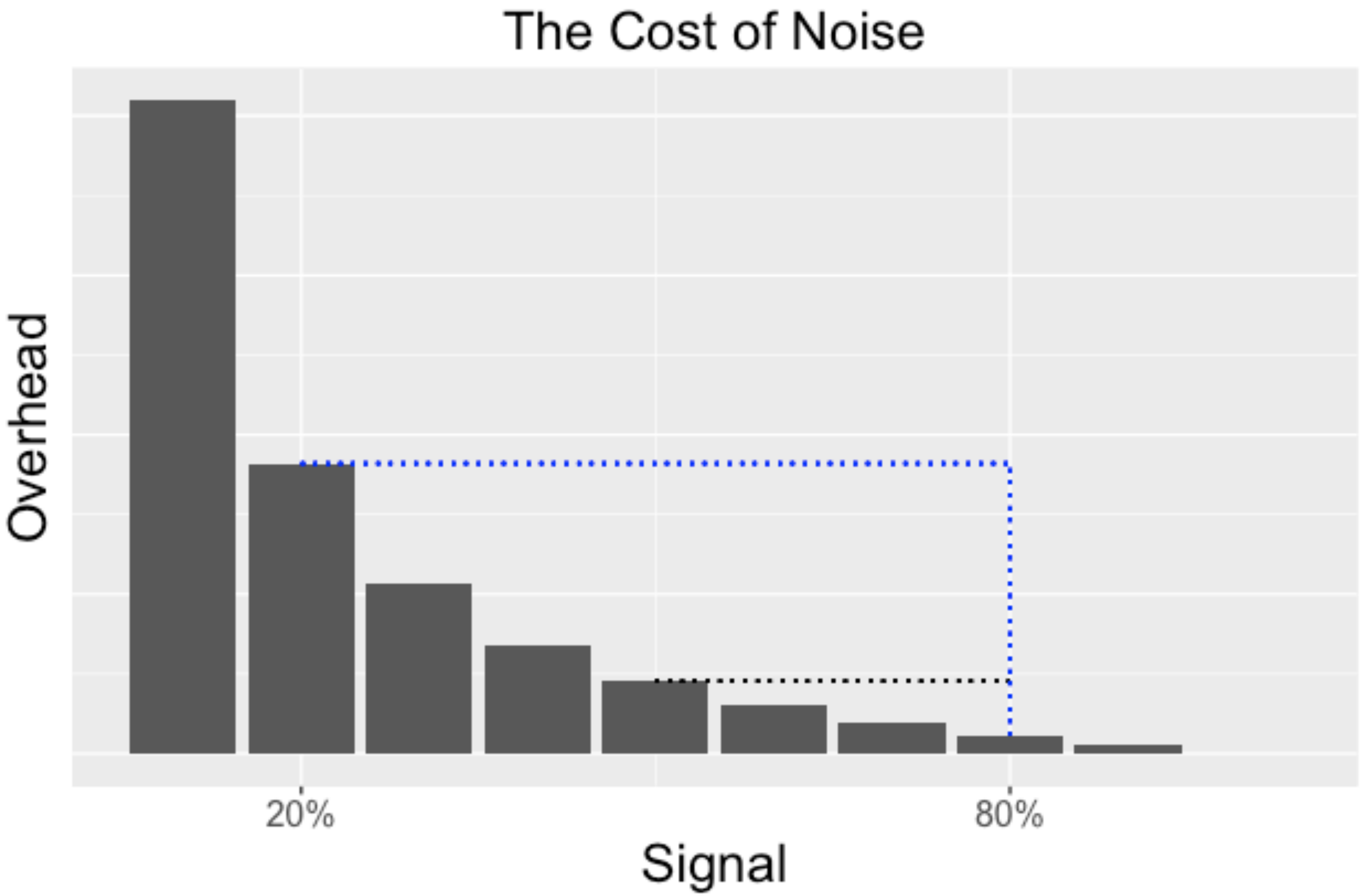


Noise increases cost of discovery and reduces efficiency.

Baseline —
  Initial cost +
  Maintenance

Volume —
  Reports/day,
  Percent valid

Triage —
  Reports/hour,
  Hourly rate



Filters

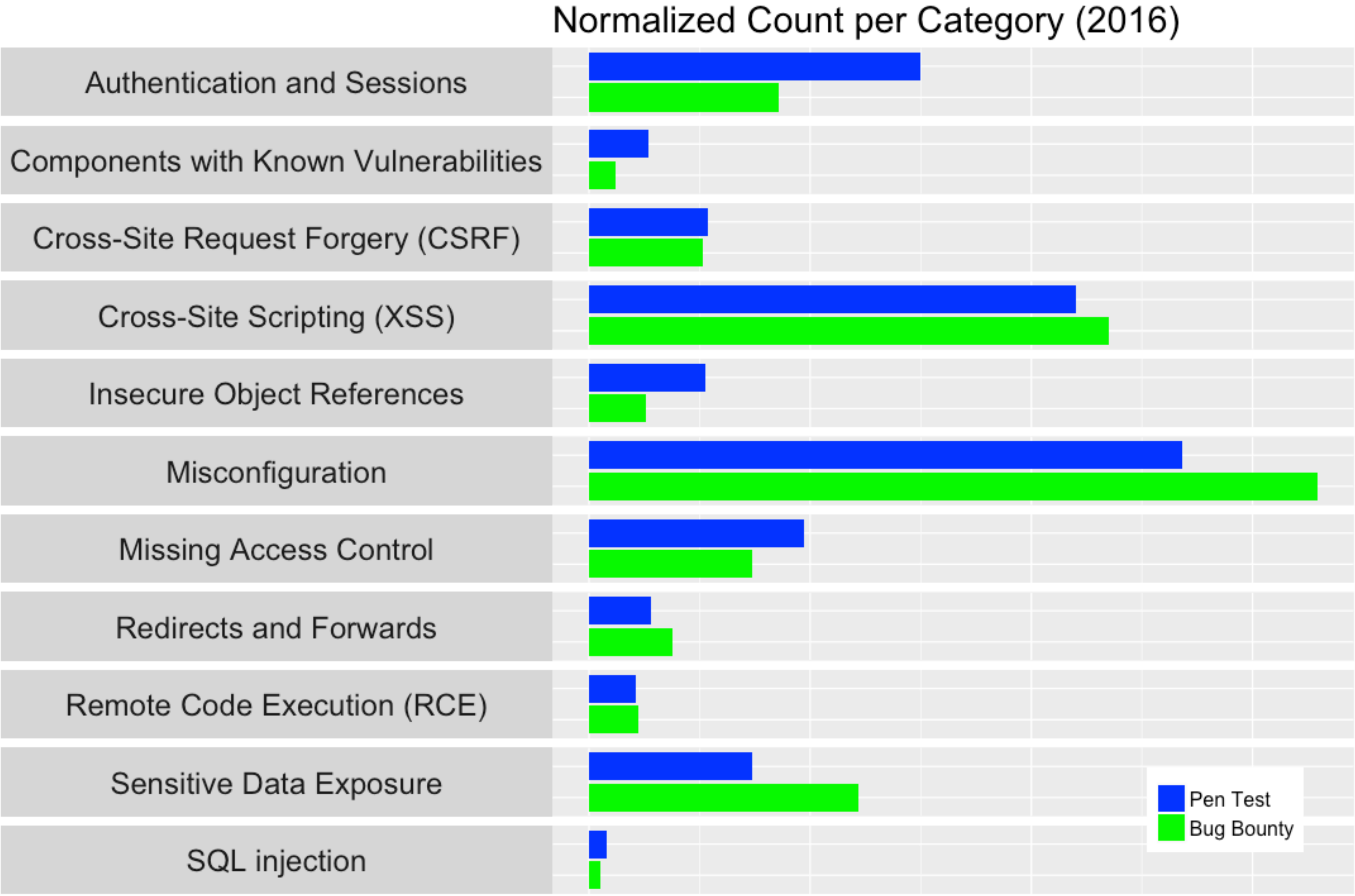
Clear, concise documentation

Scope*

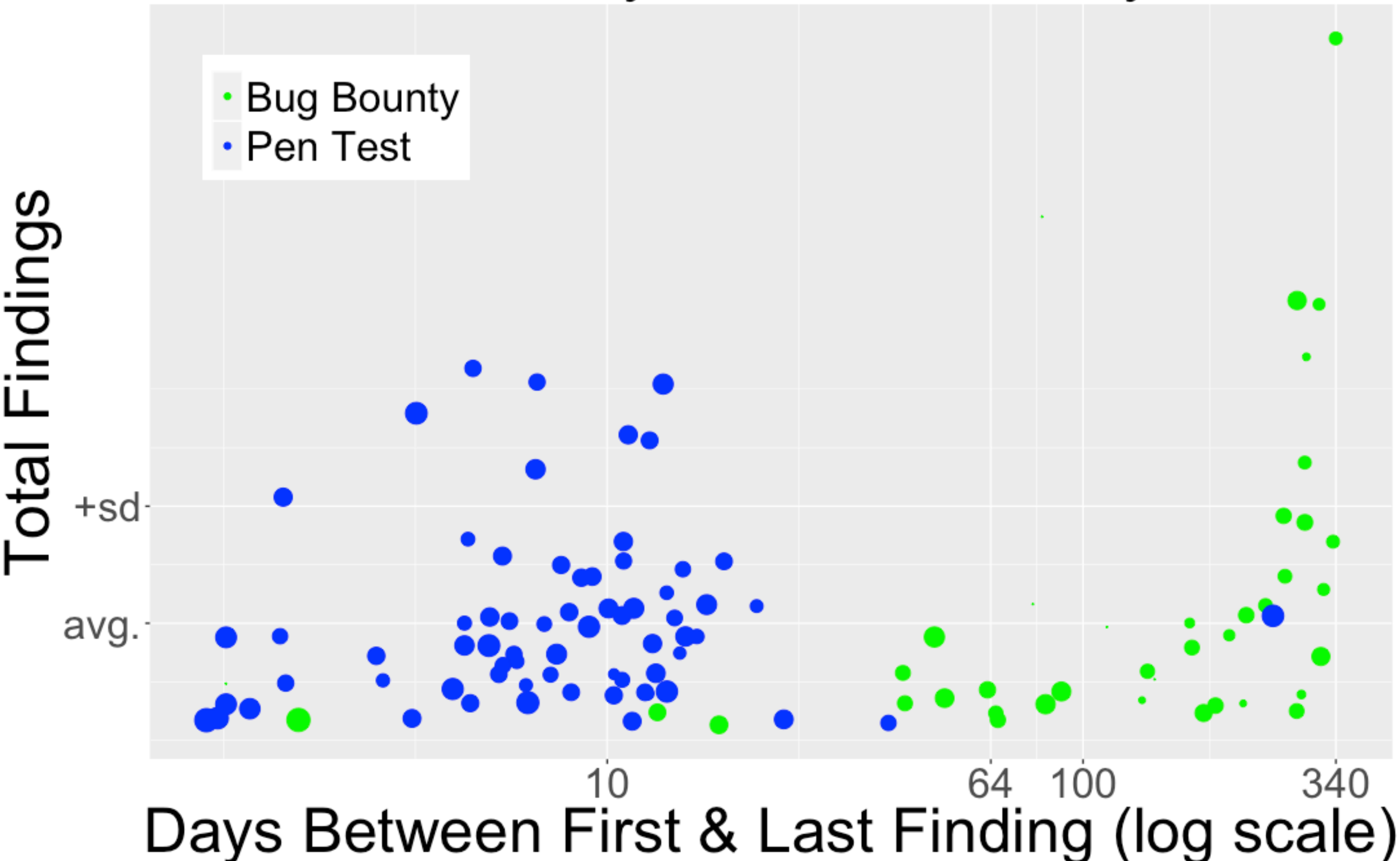
Rules of engagement*

Practical SLAs for responses

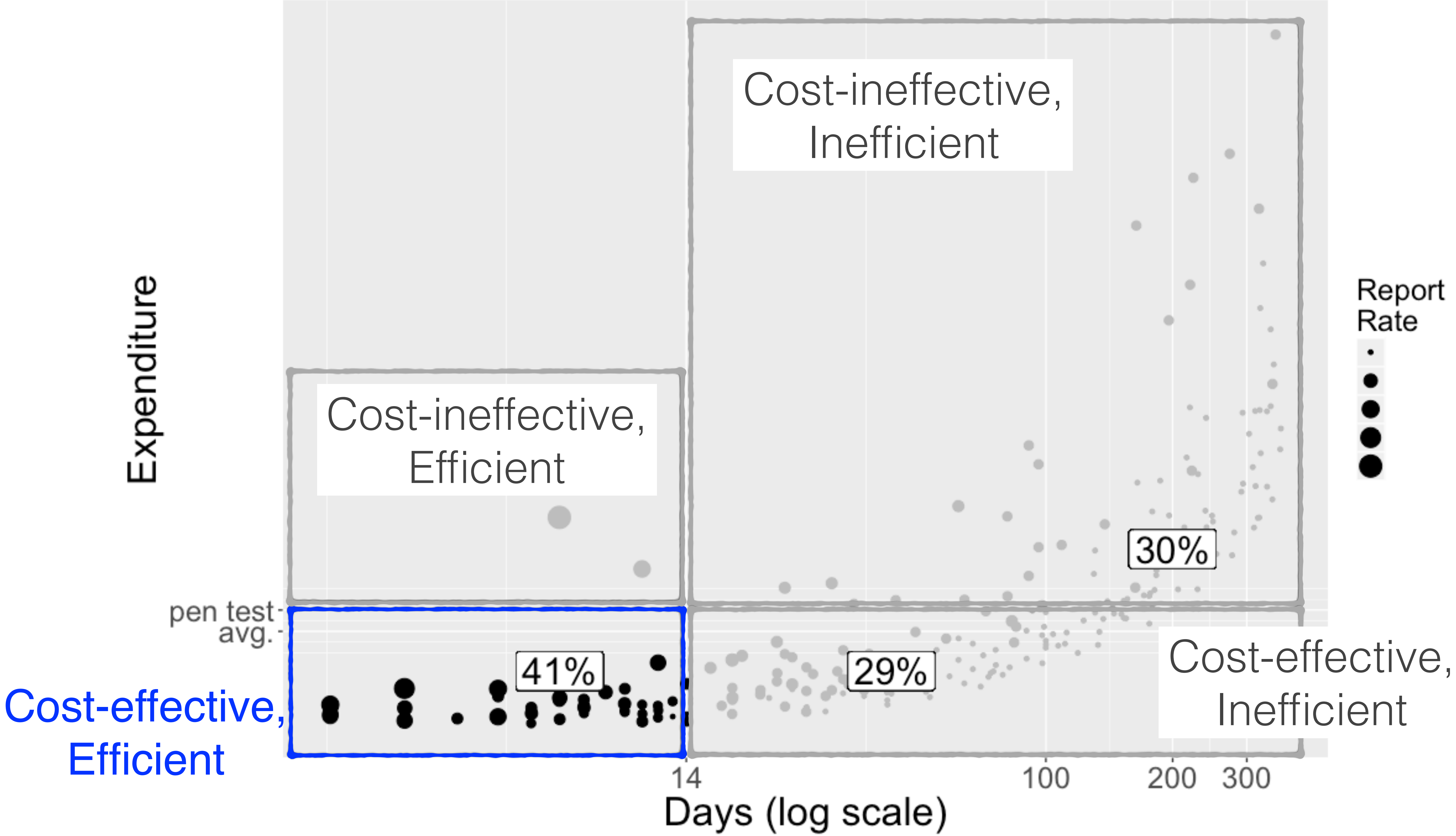
Expectations of reasonable threat models


Normalized Count per Category (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 Vuln Discovery



Vuln Discovery Cost



Cost-ineffective, Inefficient

Cost-ineffective, Efficient

Cost-effective, Efficient

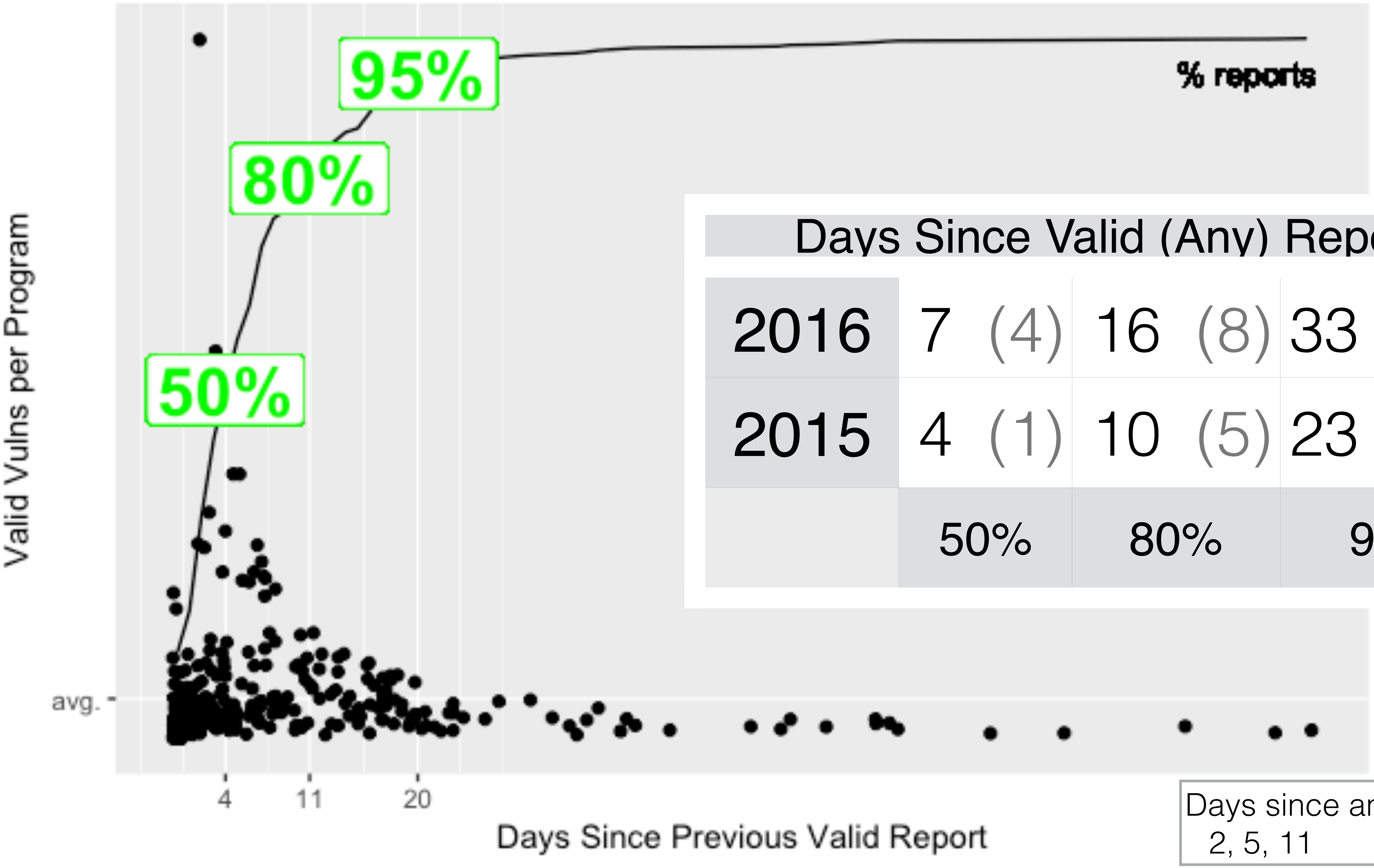
Cost-effective, Inefficient

Where are the scanners?

Overlaps, gaps, and ceilings in capabilities.

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

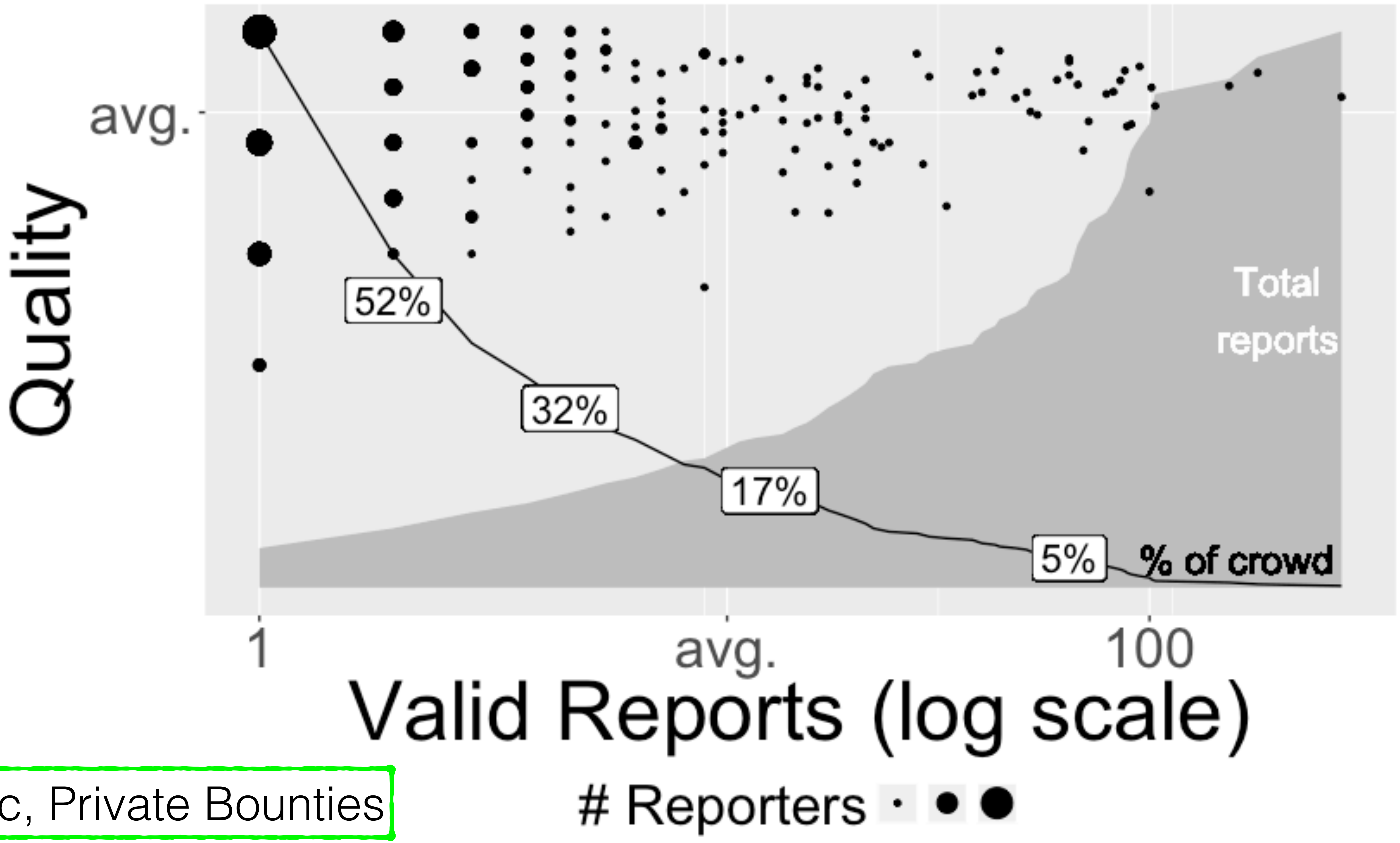
Exhausting the Pace of Vulns...or Attention?



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

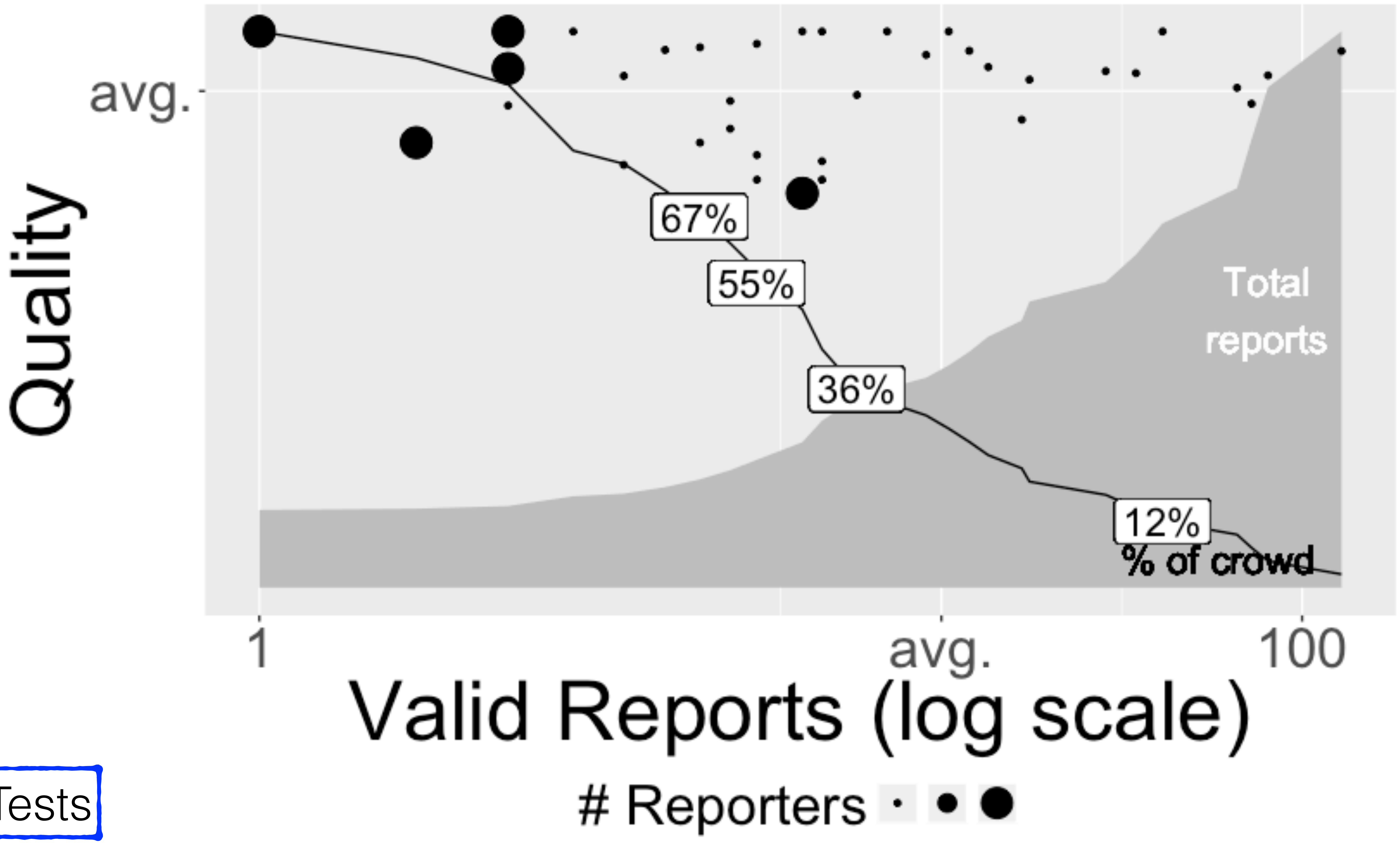
Days since any report:
2, 5, 11

The Crowd's Hoard



Public, Private Bounties

The Crowd's Hoard



Pen Tests

> “We’ll always have bugs.
> Eyes are shallow.”

– Mike’s Axiom of AppSec

BugOps vs. DevOps

Chasing bugs isn't a strategy.

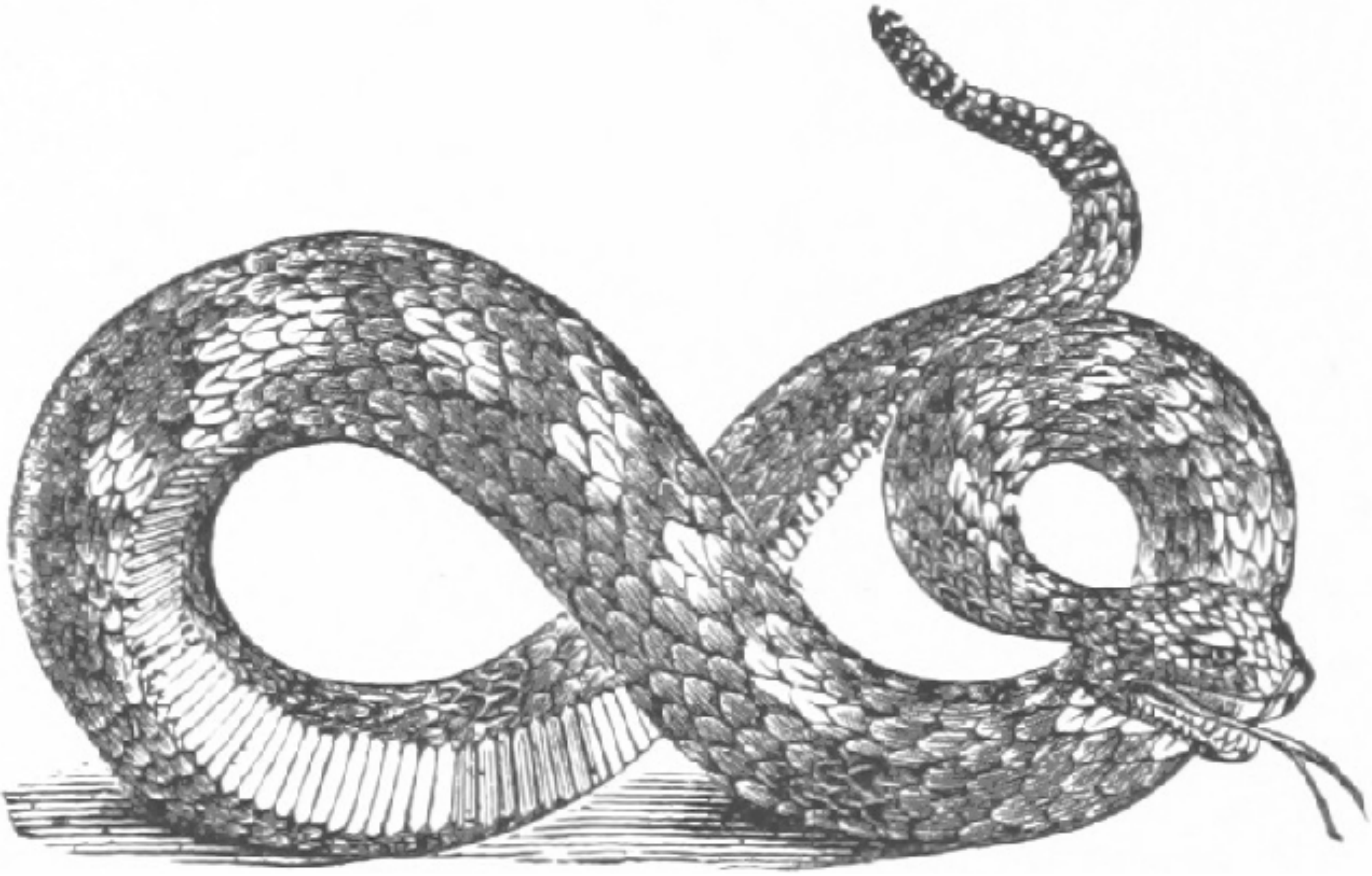
Where is threat modeling?

DevOps exercise guided by security.

Influences design.

Informs implementation.

Increases security awareness.



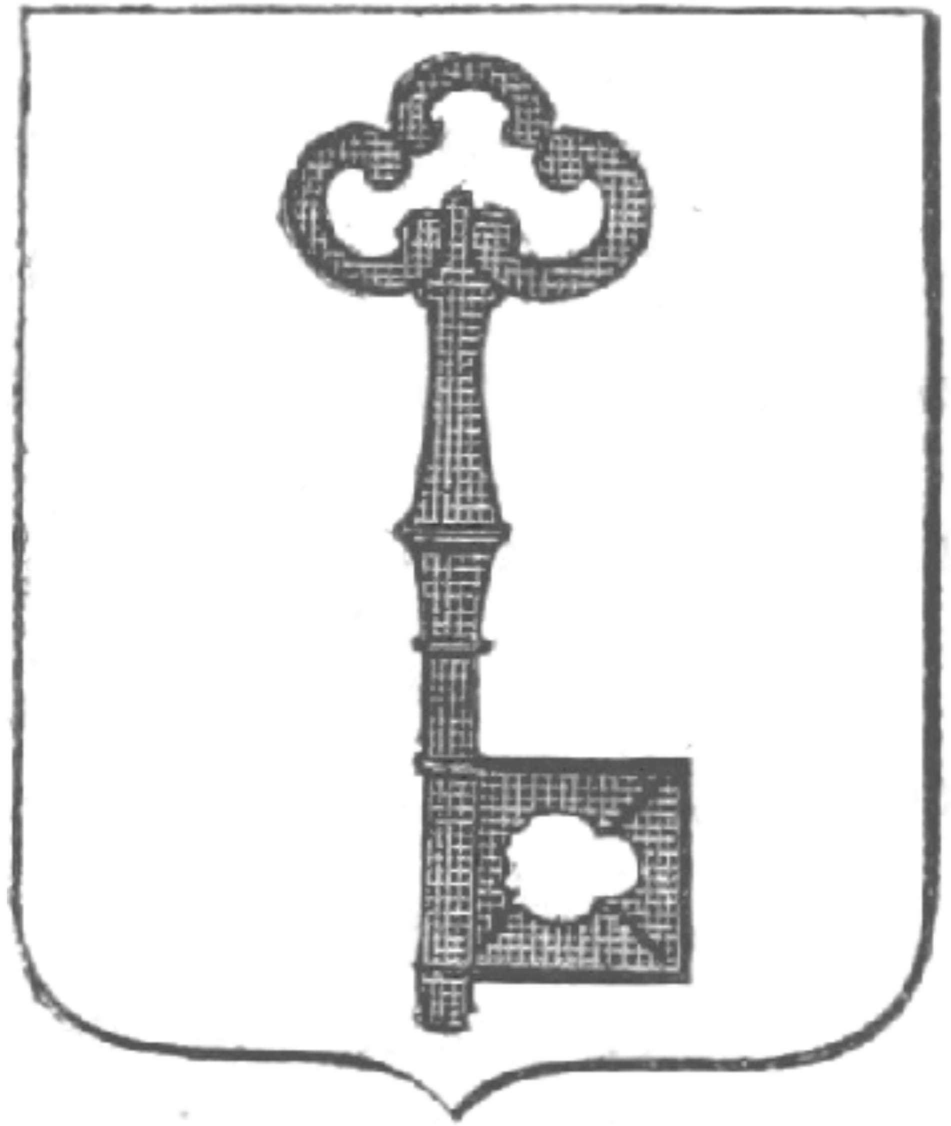
Risk reduction.

“You’re not using HTTPS.”

“Use HTTPS.”

“Seriously. Please use HTTPS.”

Let’s Encrypt.

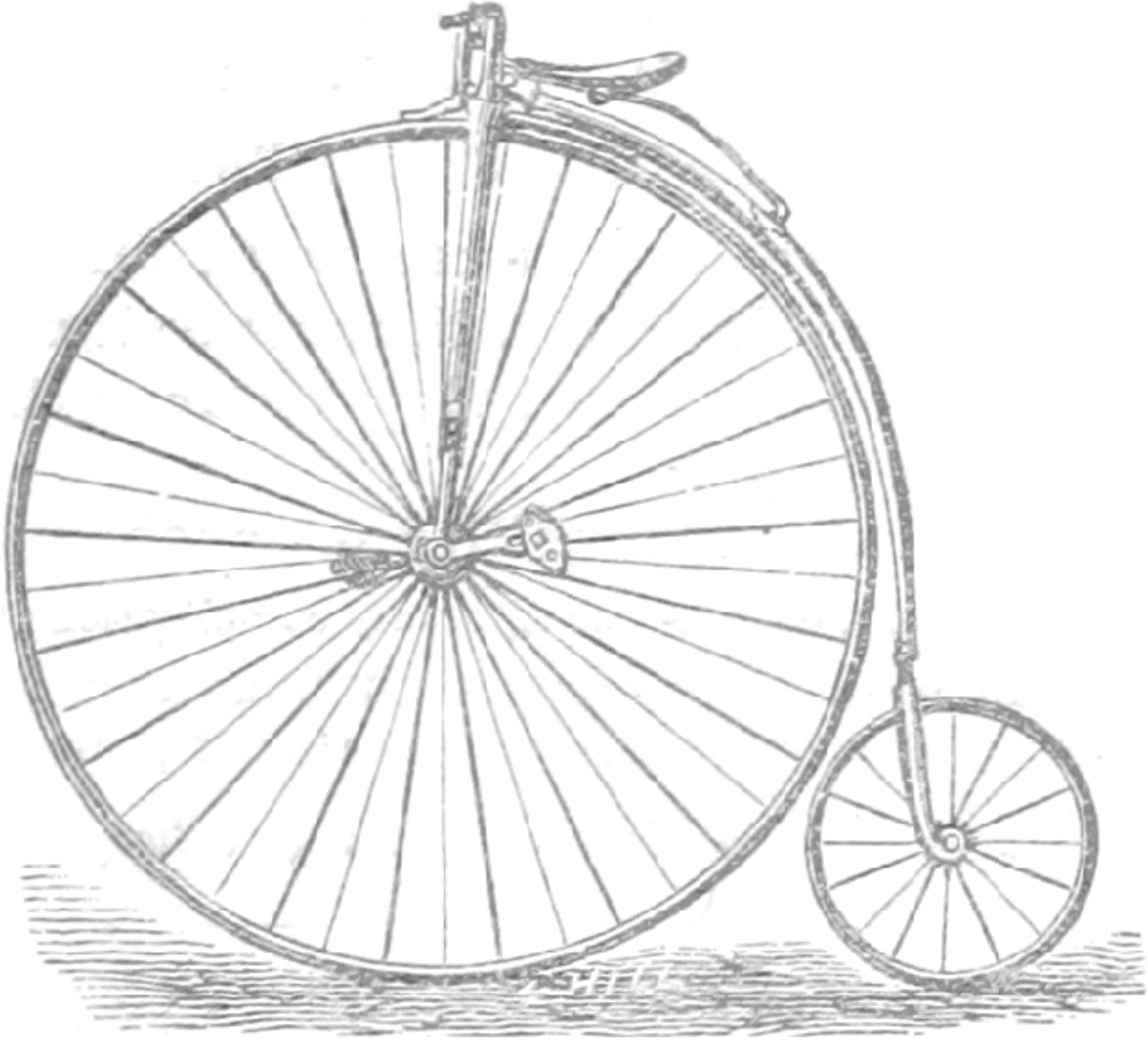


Risk Strategies

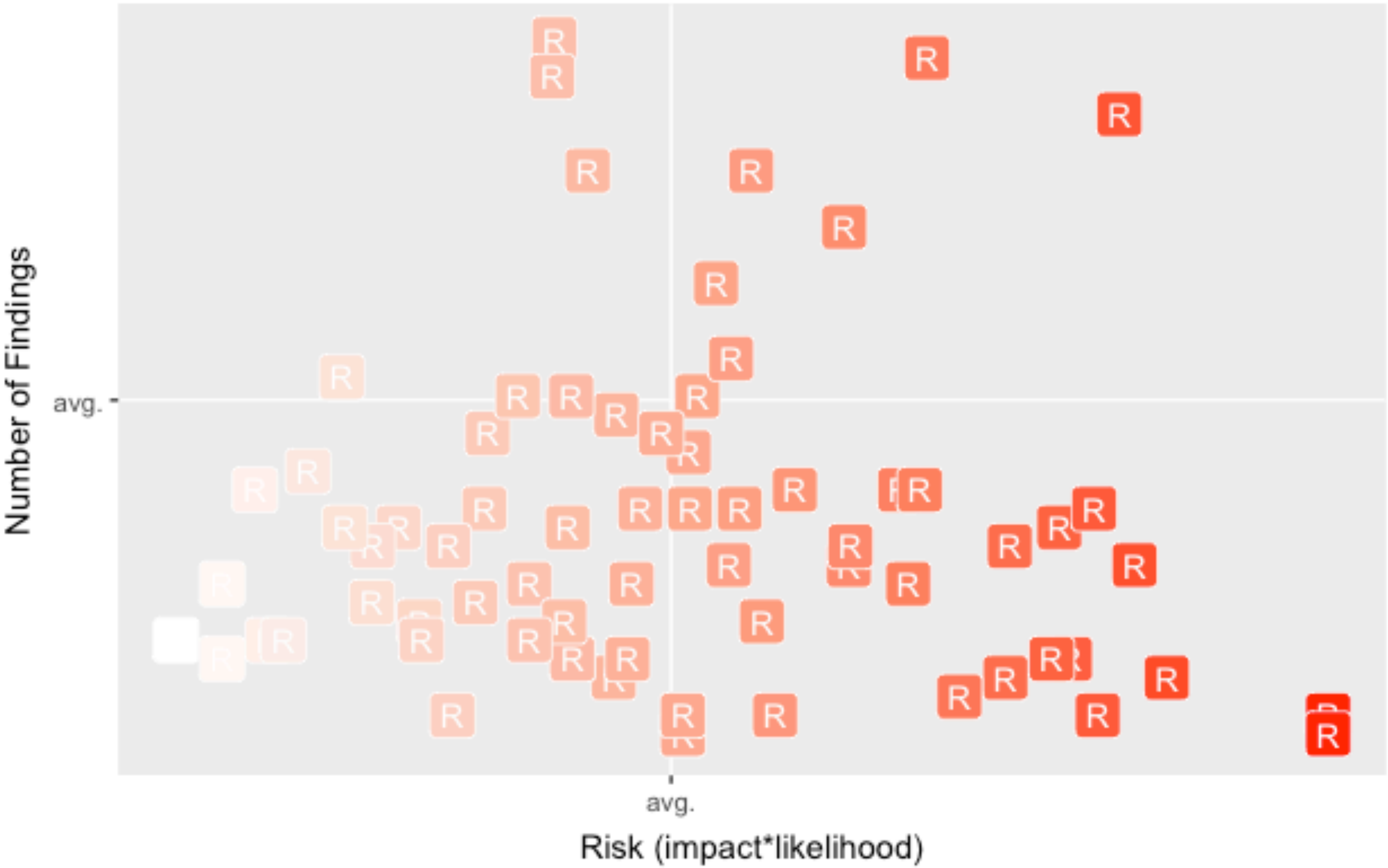
Decrease rate of reports for ___ vulns.

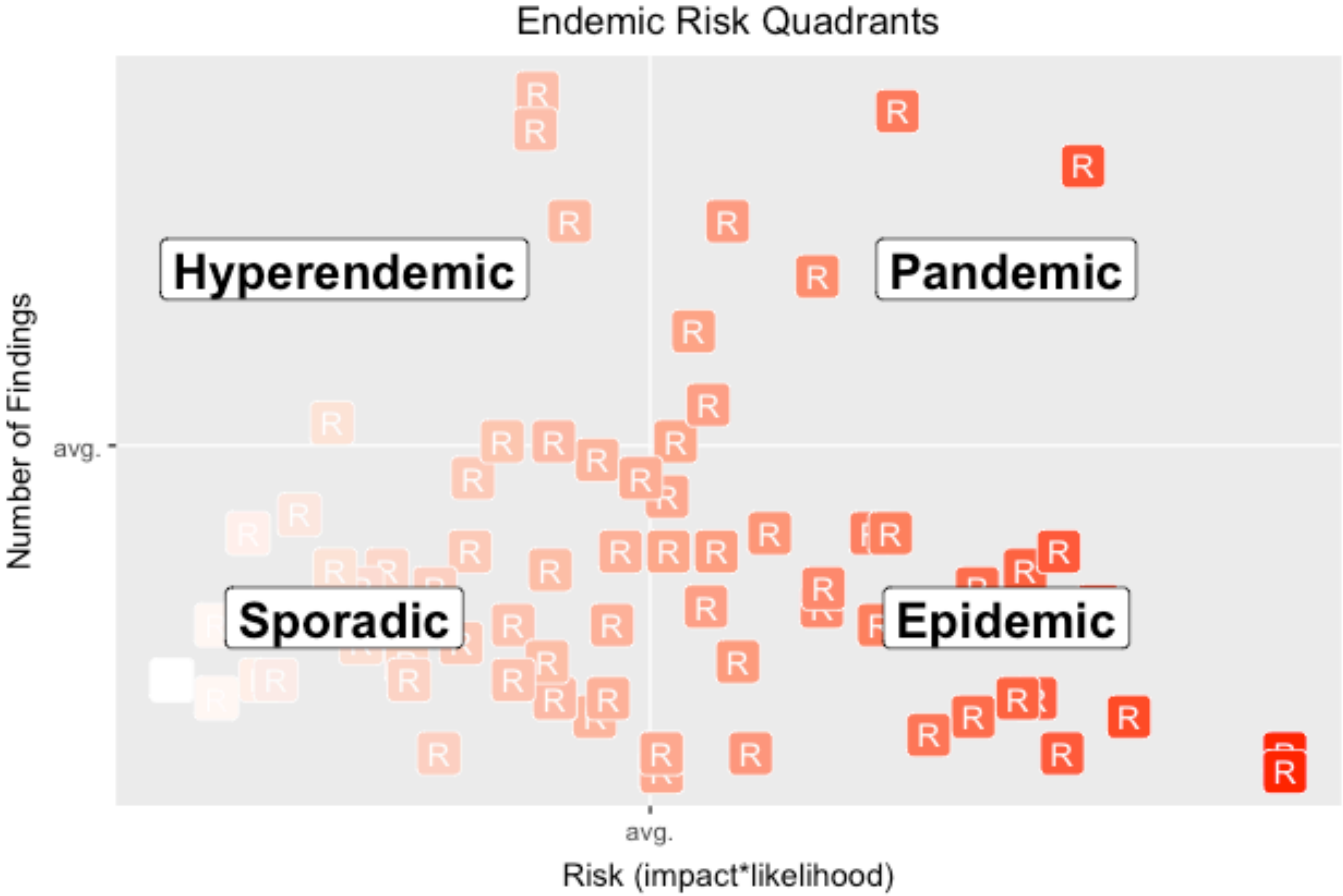
Increase speed of deploying fixes for ___ vulns.

Deploy ___ to counter category of ___ vulns.



Risk vs. Findings per Pen Test (2016)




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

Bounty ranges as a proxy for SDL, where price implies maturity.

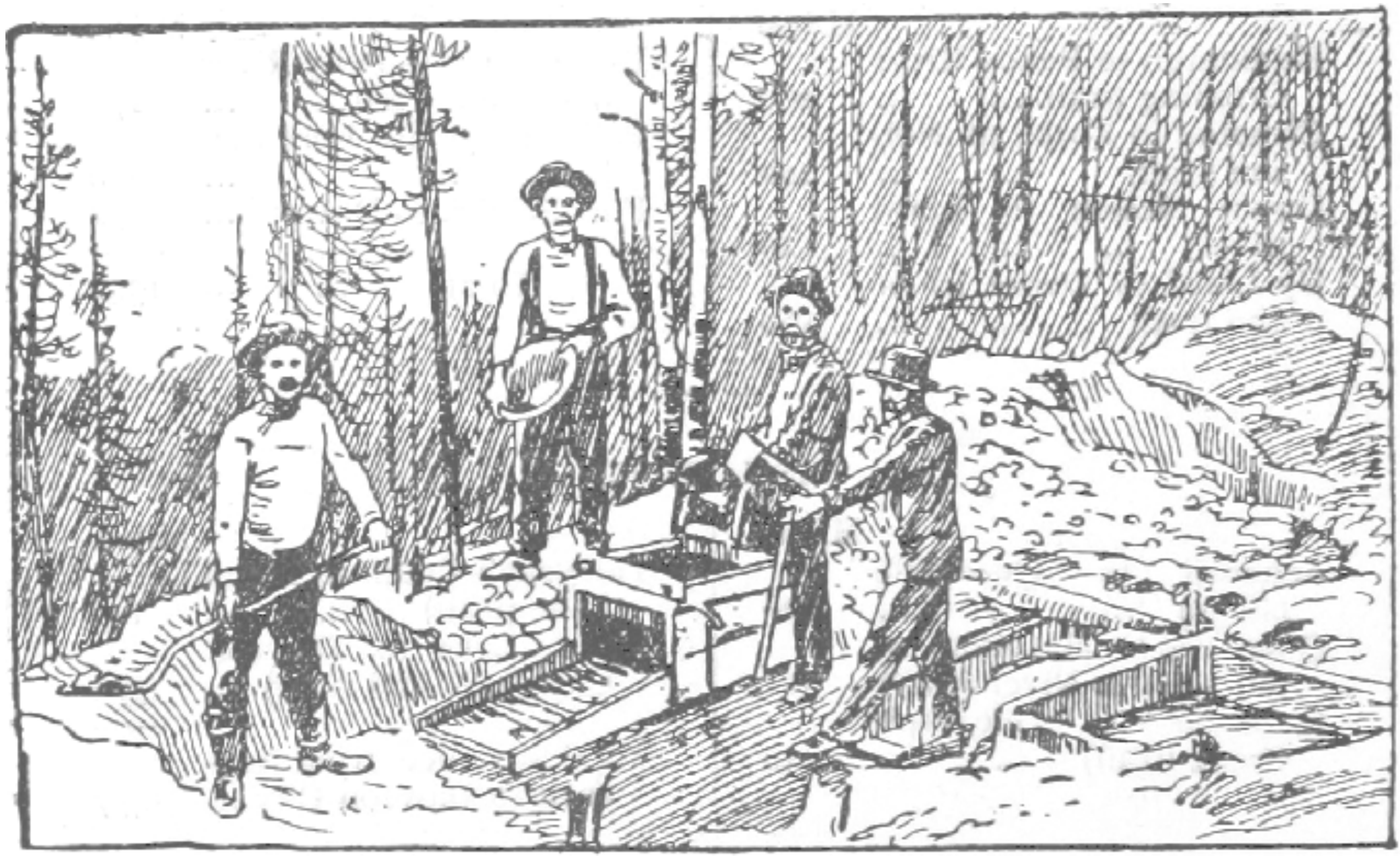
$	1	Experimenting
$	1,000	Enumerating
$	10,000	Exterminating
$	100,000	Extinct-ifying

Bounties

Based on realistic threat models.

Incentivized quality and effort.

Machine-readable reports.



Crowds

Public bounty

Private bounty

Pen testing

Threat intel sharing

Fuzzing farms

Create threat models.

Measure vuln discovery effort.

Strive for automation.

Thank You!

blog.cobalt.io

Questions?

(ISC)^2 Community — http://bit.ly/4416GBU

R —
www.r-project.org

RStudio —
www.rstudio.com

`data.table`

`ggplot`