DevSecCon | LONDON
19-20 OCT 2017

The Flaws in Hordes,
The Security in Crowds

MIKE SHEMA
MIKE@COBALT.IO

Join the conversation #DevSecCon

“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.”

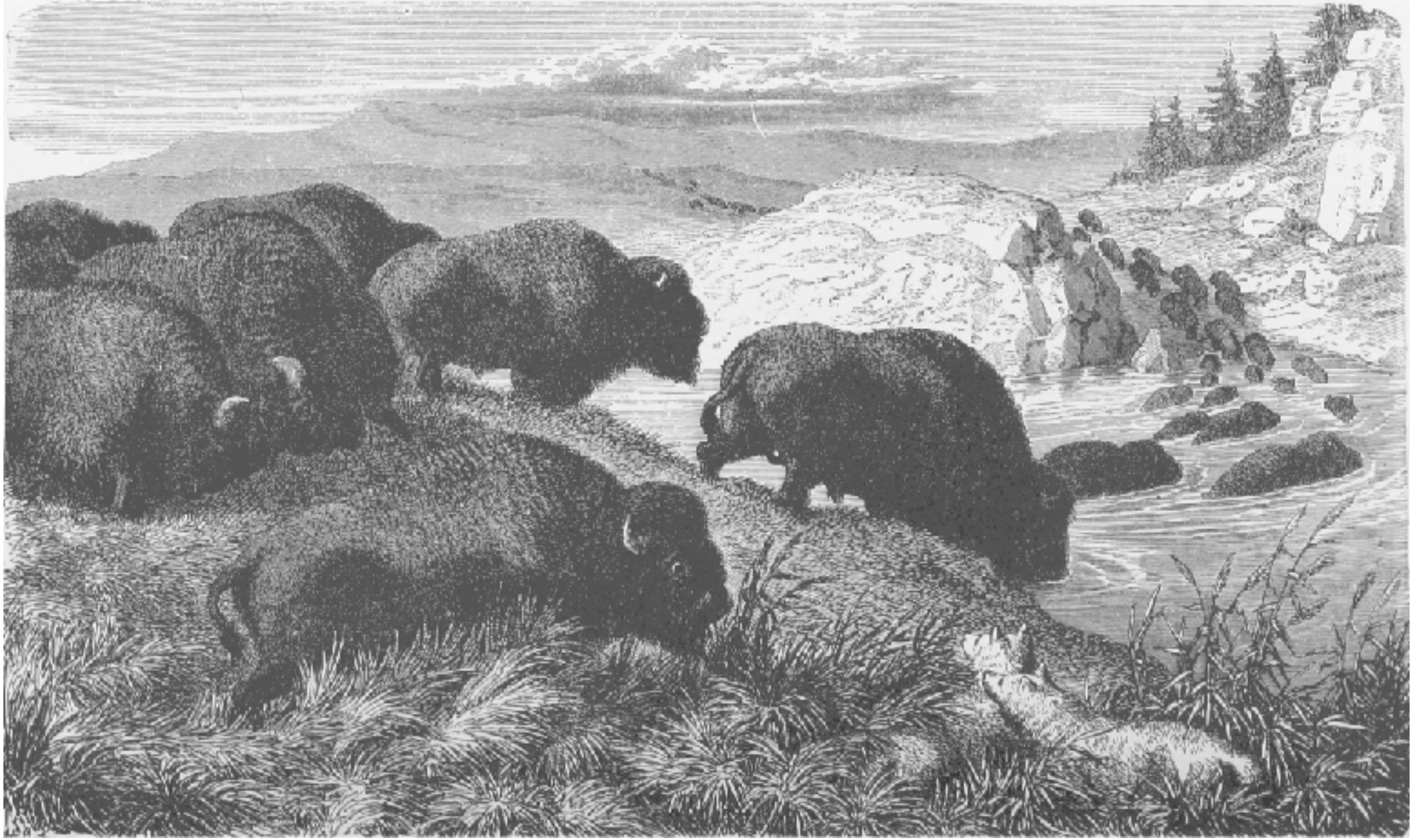
– Eli Wallach, *The Good, the Bad, and the Ugly*.

Uneasy Alliances

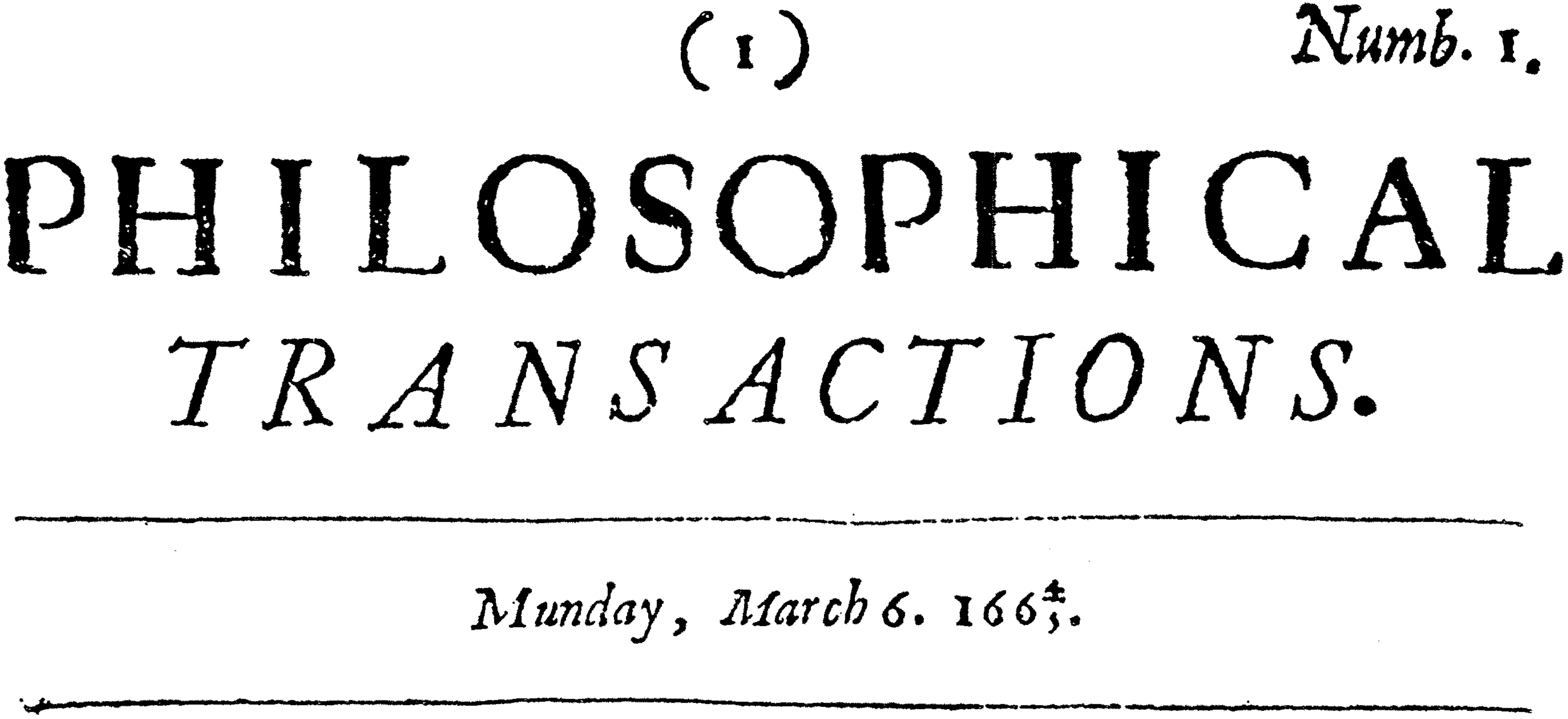
“What’s the price for this vuln?”
— Bounties

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

“What’s the value of finding vulns?”
— CSOs



Disclosure Happens



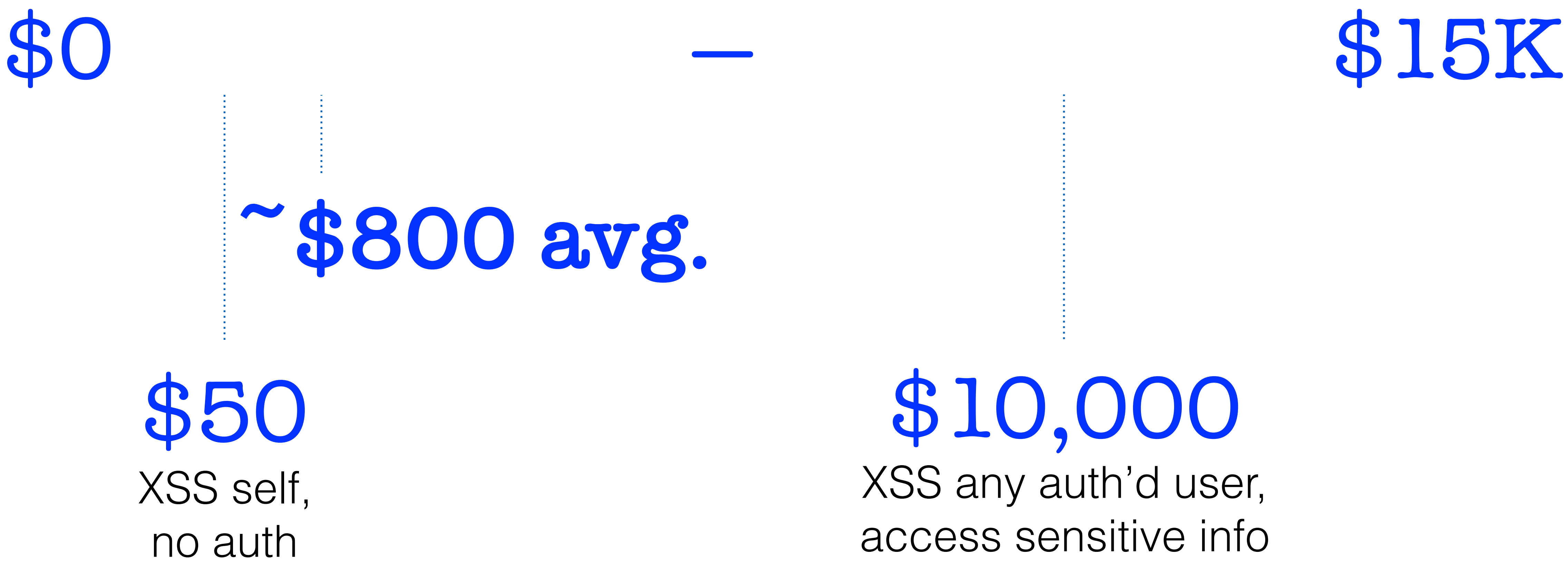
(1) Numb. 1.

PHILOSOPHICAL TRANSACTIONS.

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

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

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



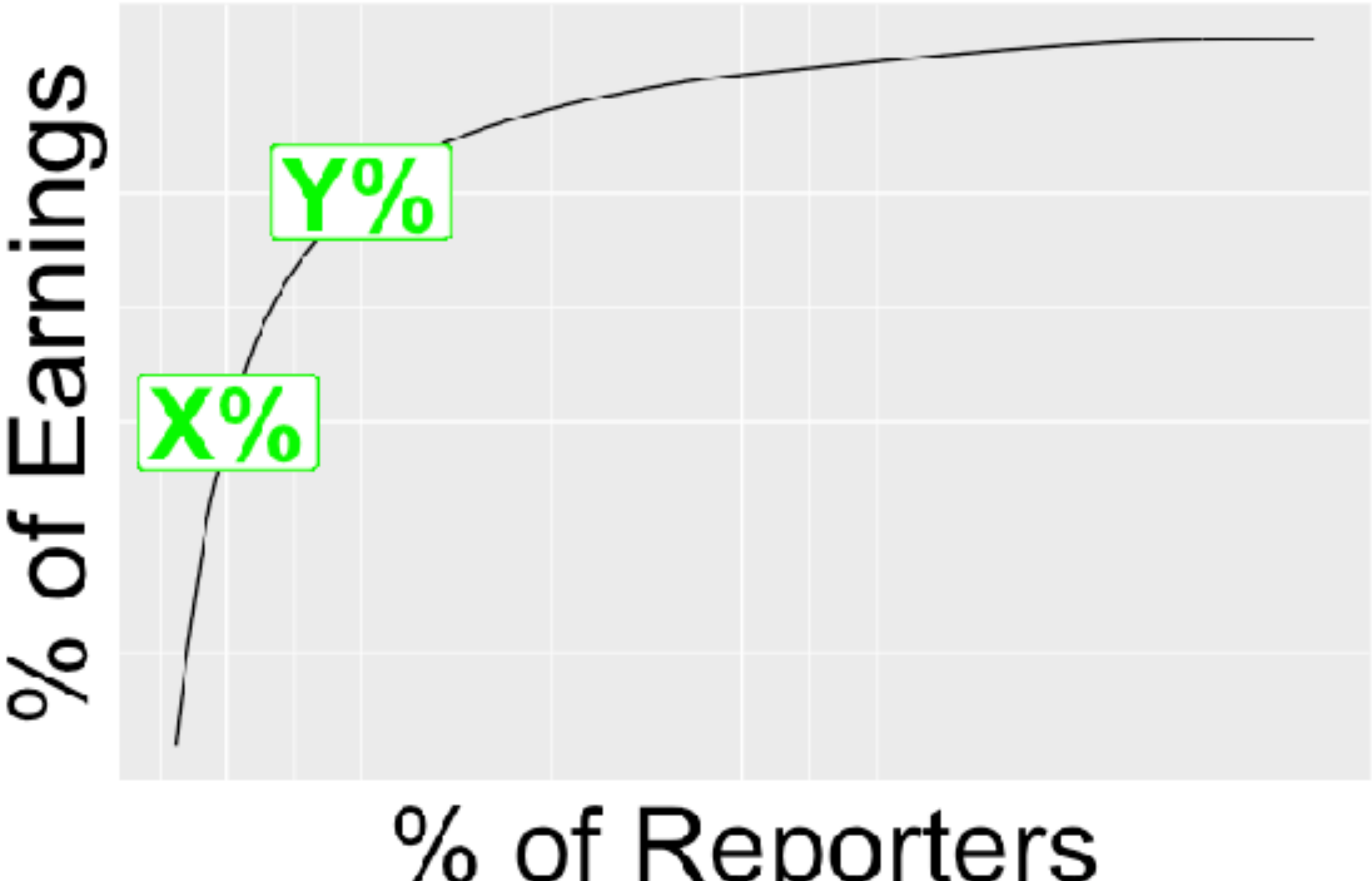
$0 – $15K

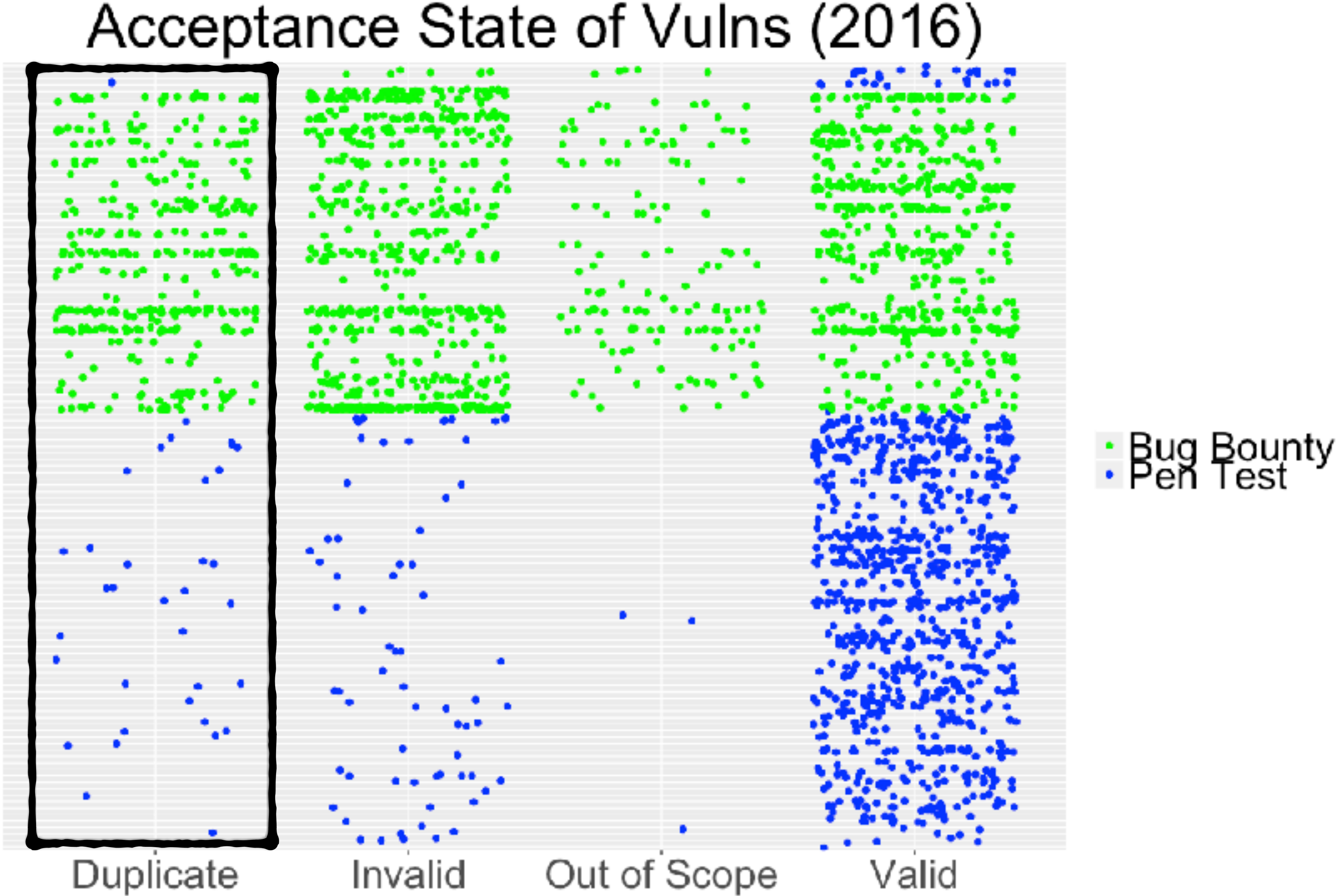
~$800 avg.

$50
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)
Duplicate
Invalid
Out of Scope
Valid
● Bug Bounty
● Pen Test

Noise increases cost of discovery and reduces efficiency.

Volume—

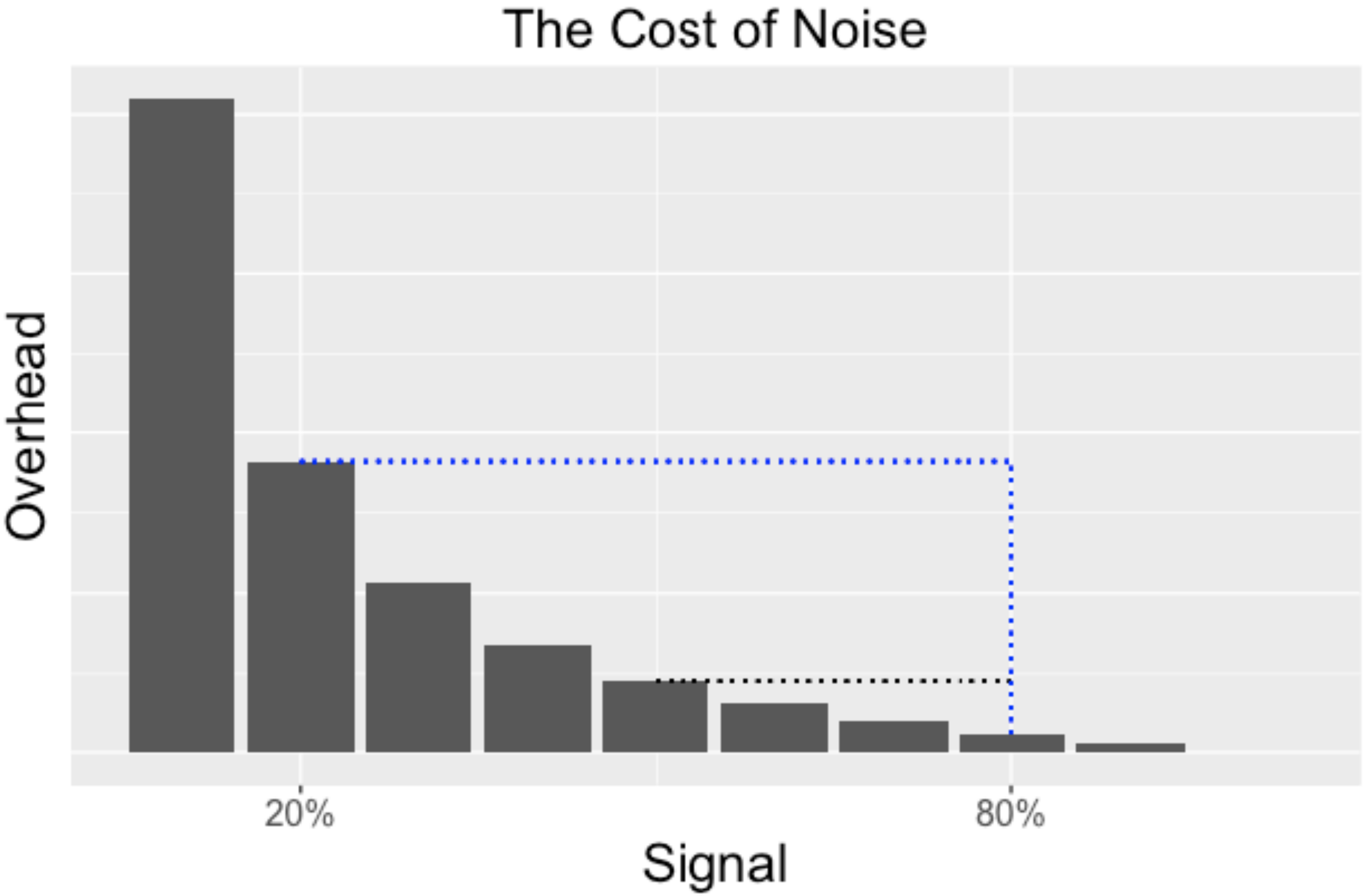
Reports/day

Percent valid

Triage—

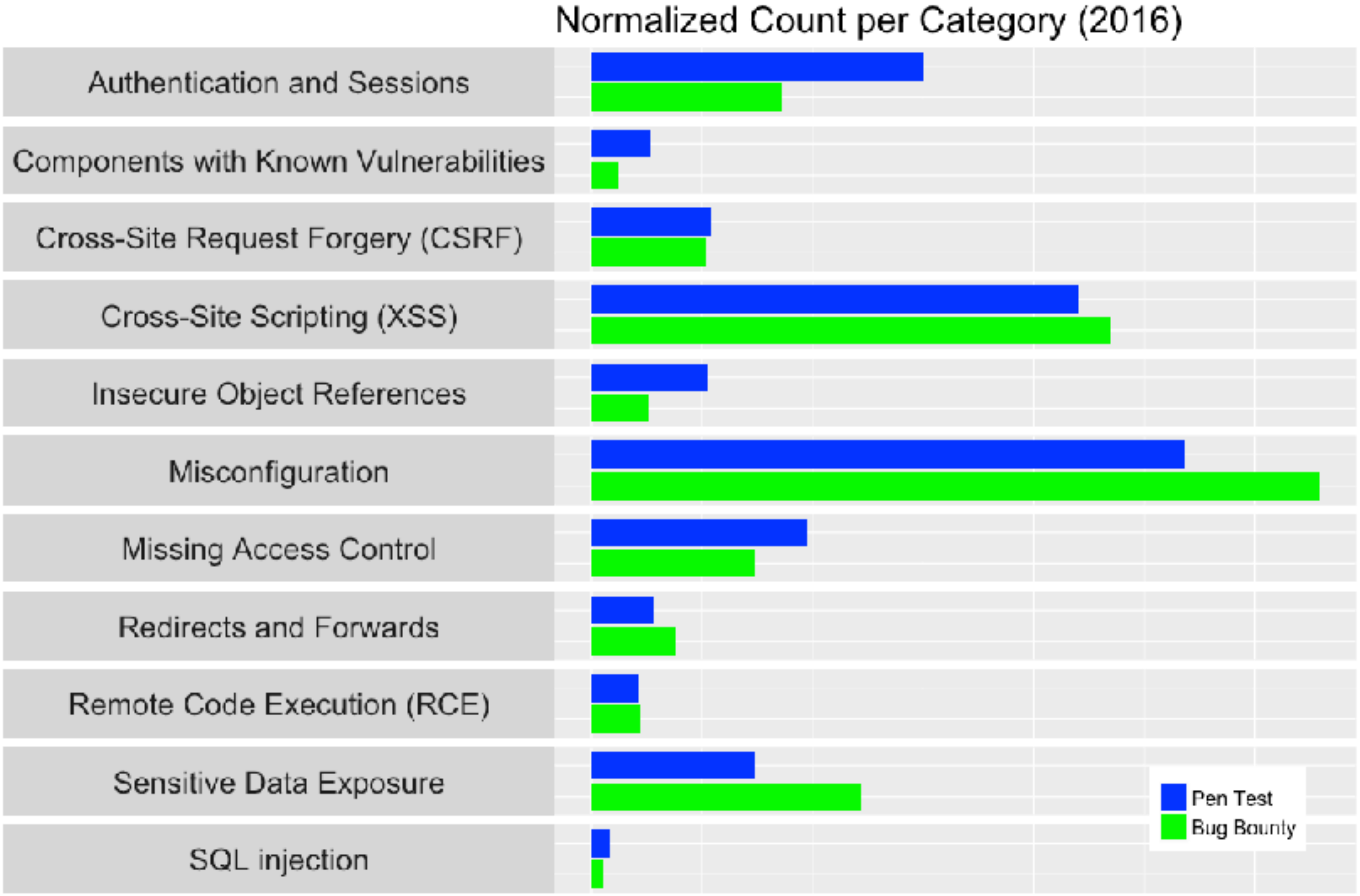
Time/report

People/report

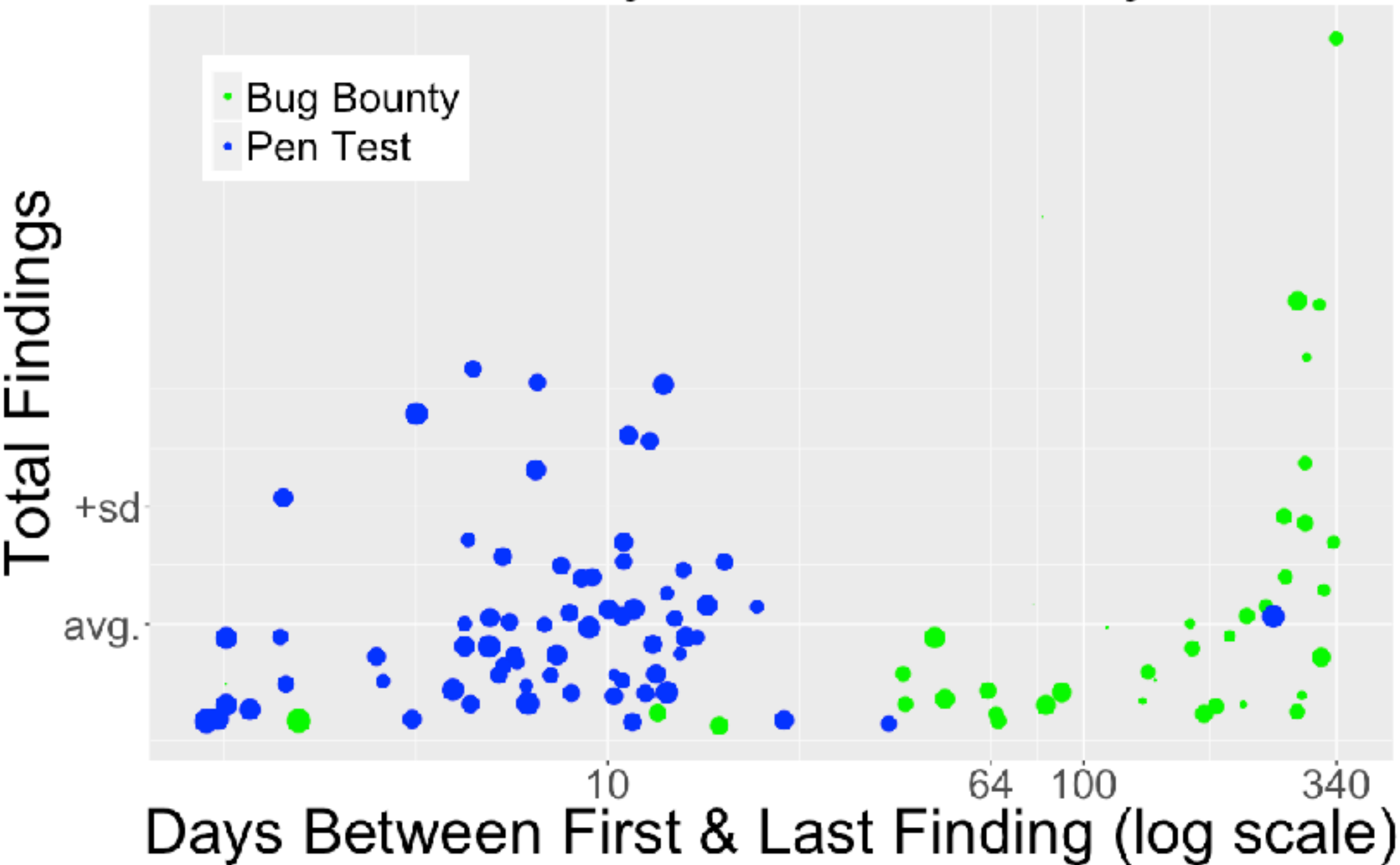


+

[Baseline]

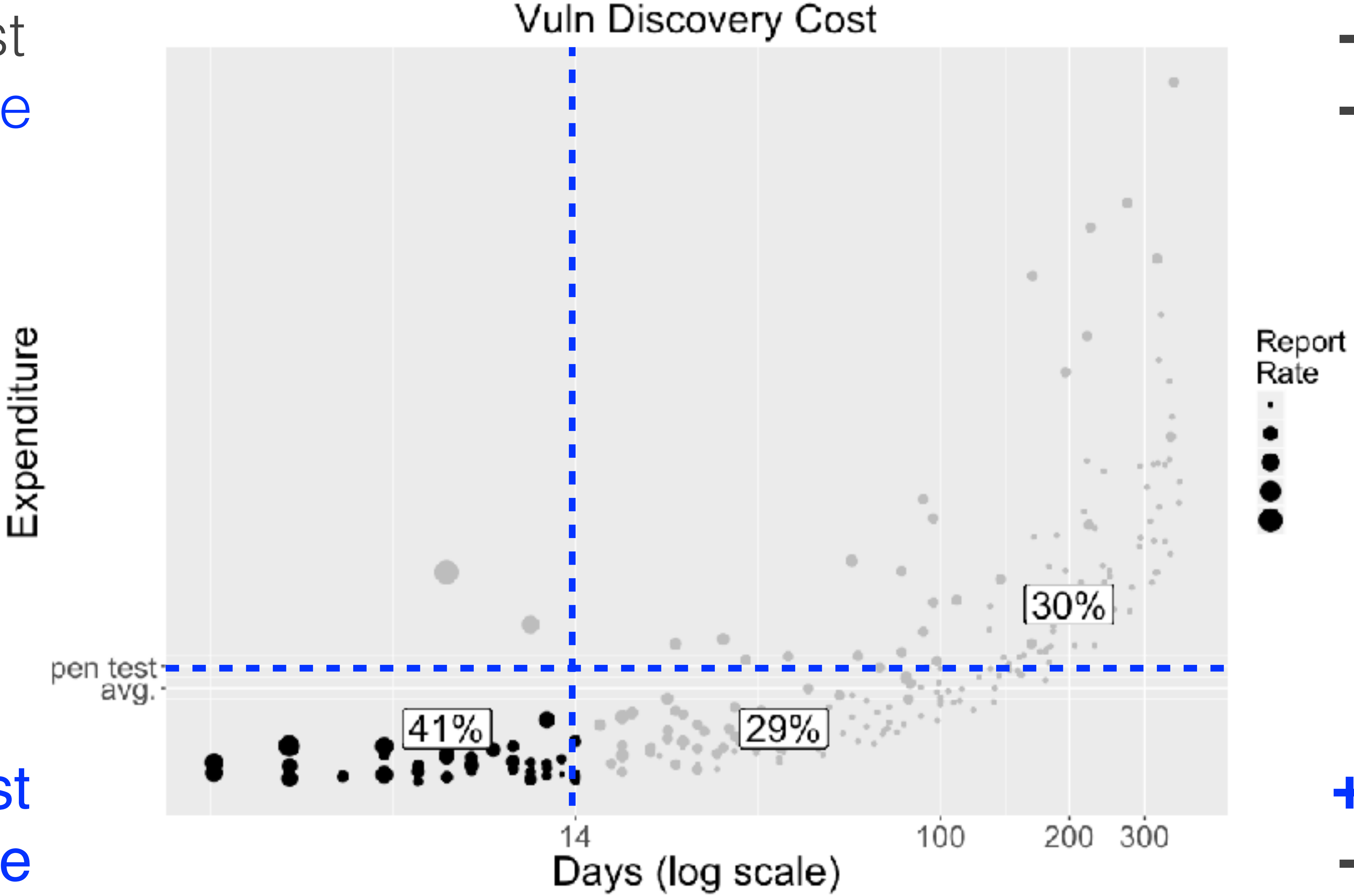

Normalized Count per Category (2016)
Authentication and Sessions
Components with Known Vulnerabilities
Cross-Site Request Forgery (CSRF)
Cross-Site Scripting (XSS)
Insecure Object References
Misconfiguration
Missing Access Control
Redirects and Forwards
Remote Code Execution (RCE)
Sensitive Data Exposure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

Efficiency of Vuln Discovery



-cost
+time

-cost
-time



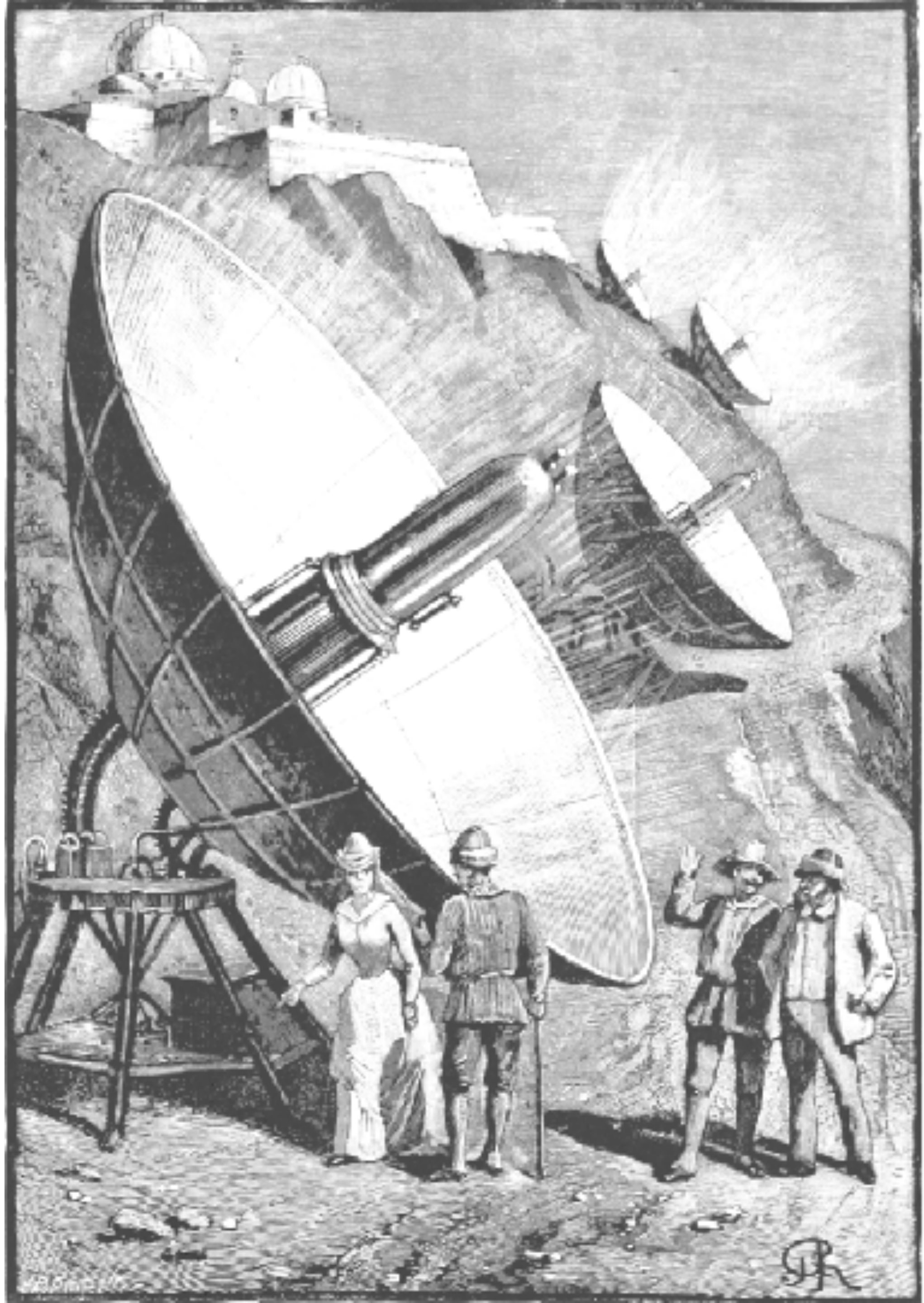
+cost
+time

+cost
-time

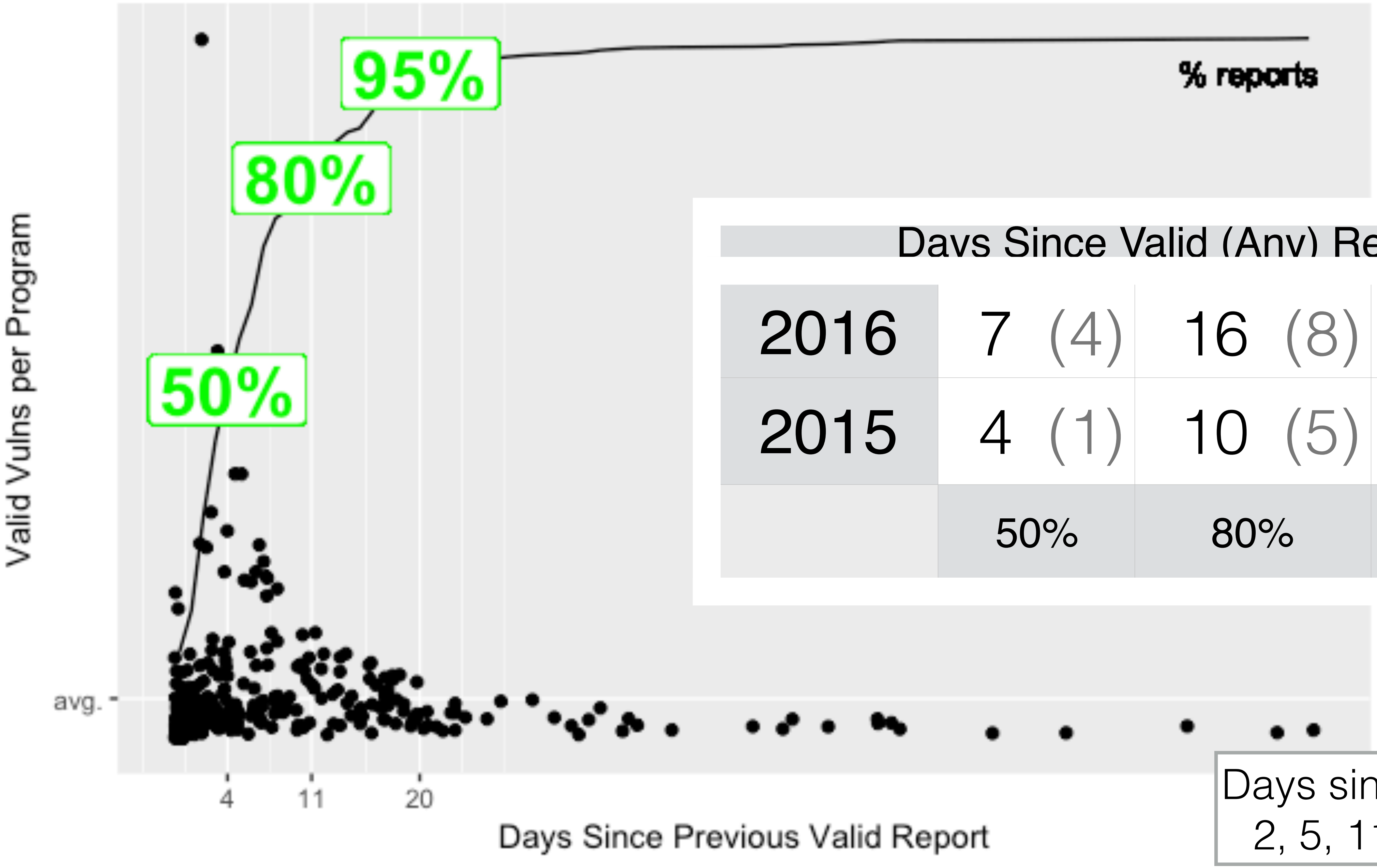
Scanners

Overlaps, gaps, and ceilings in capabilities.

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



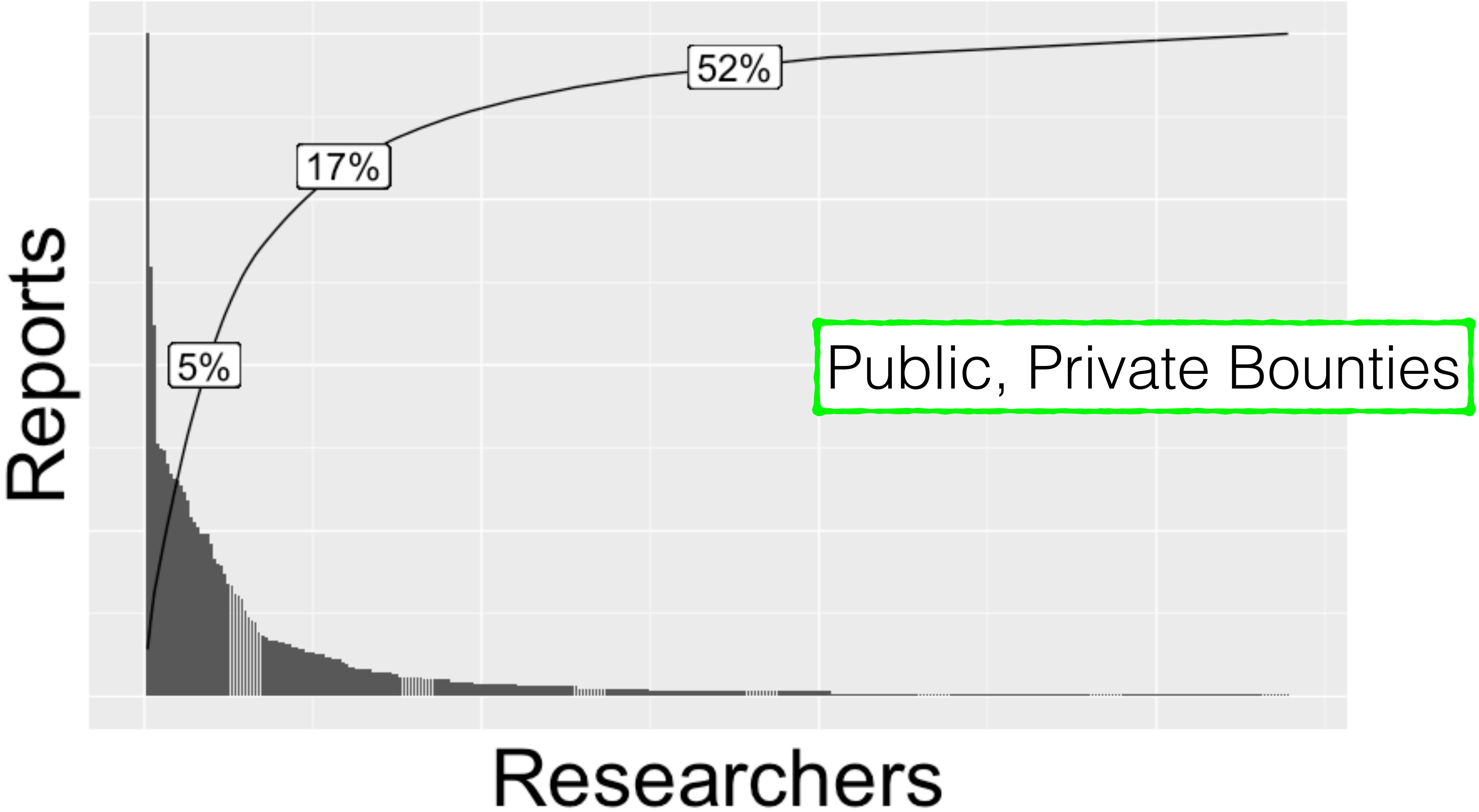
Exhausting the Pace of Vulns...or Attention?



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

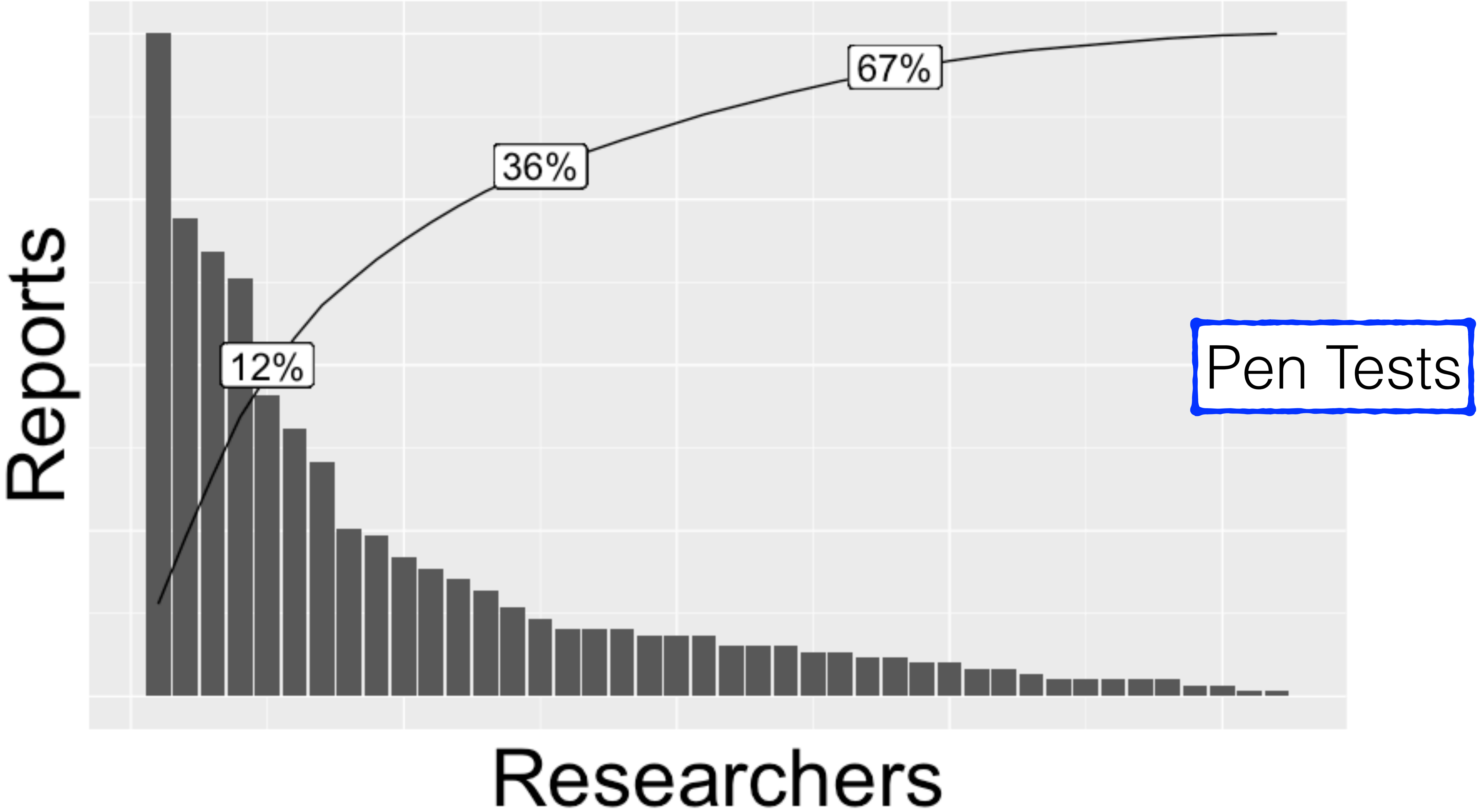
Days since any report:
2, 5, 11

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.

As we move to security as code,

code moves to inevitable legacy.

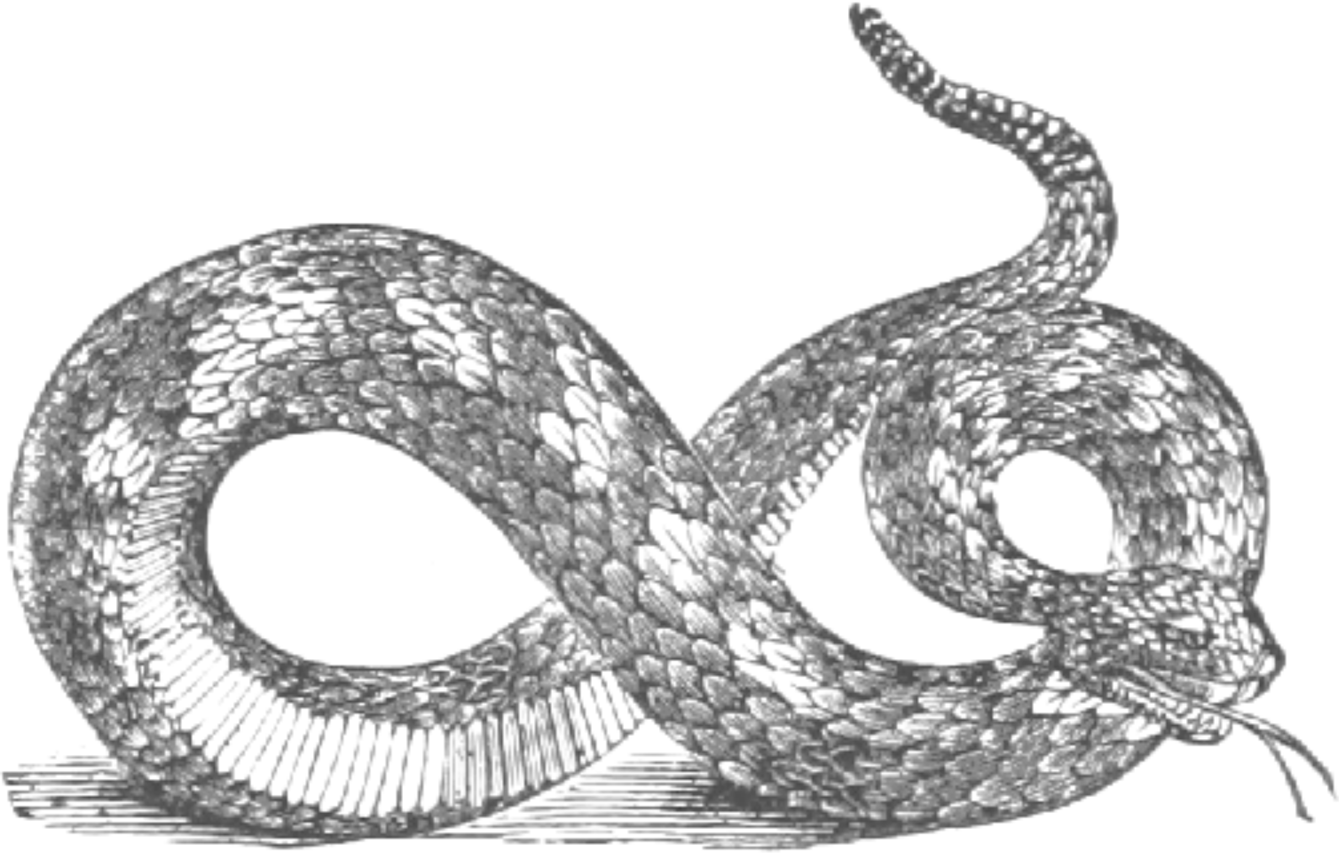
Threat Modeling

DevOps exercise guided by security.

Influences design.

Informs implementation.

Increases security awareness.



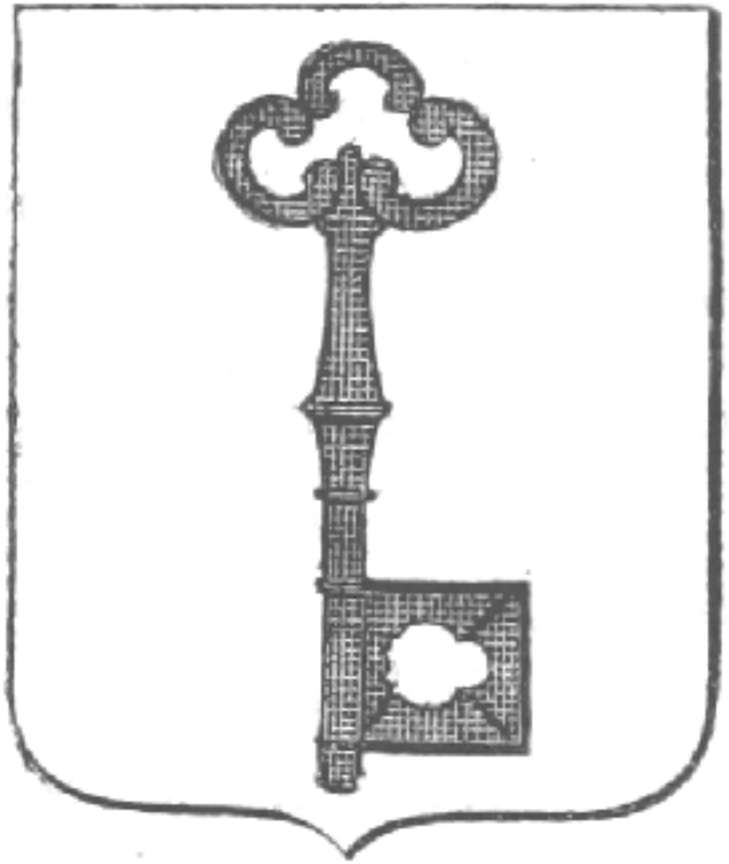
Risk Reduction

“You’re not using HTTPS.”

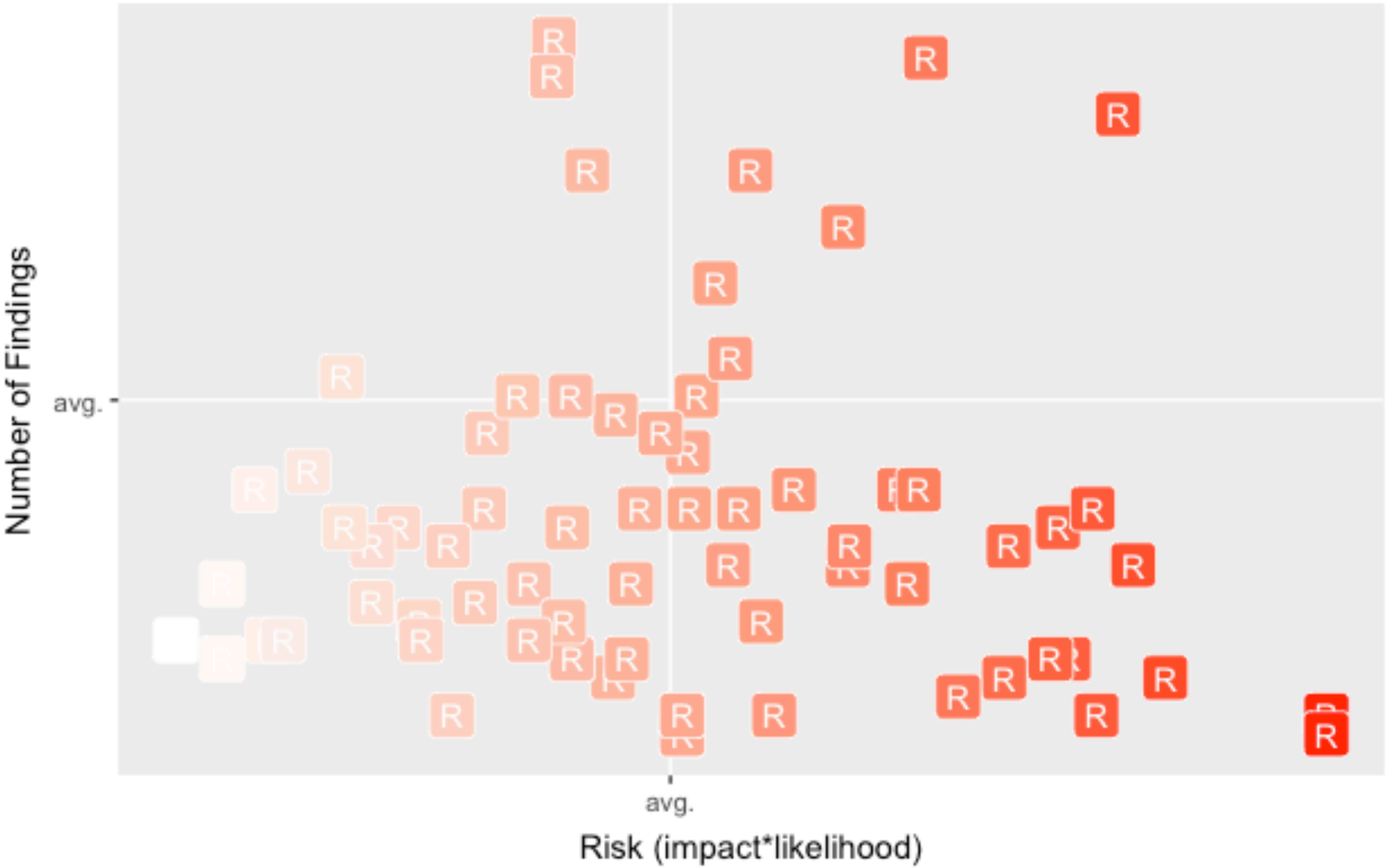
“Use HTTPS.”

“Seriously. Please use HTTPS.”

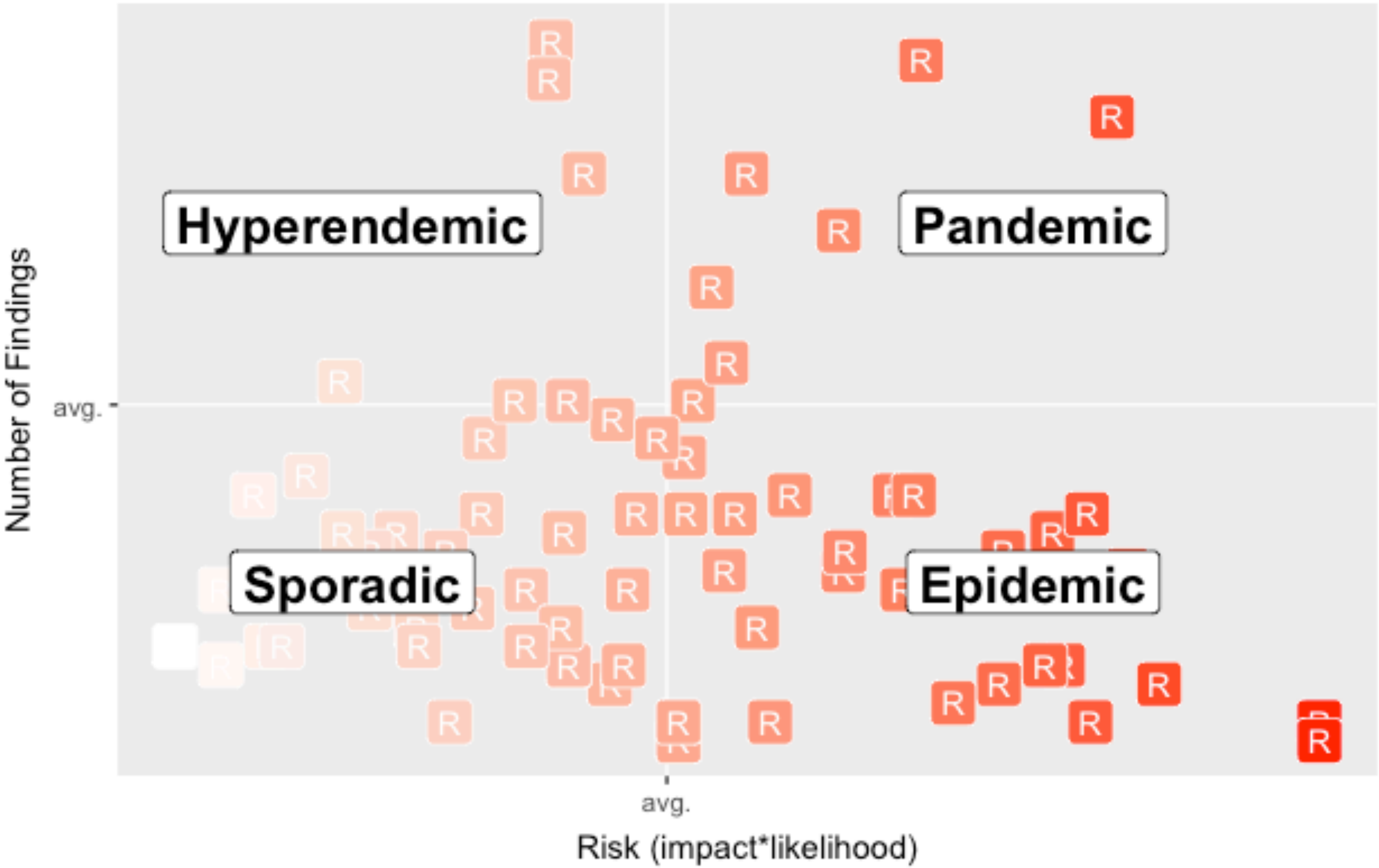
Let’s Encrypt.



Risk vs. Findings per Pen Test (2016)



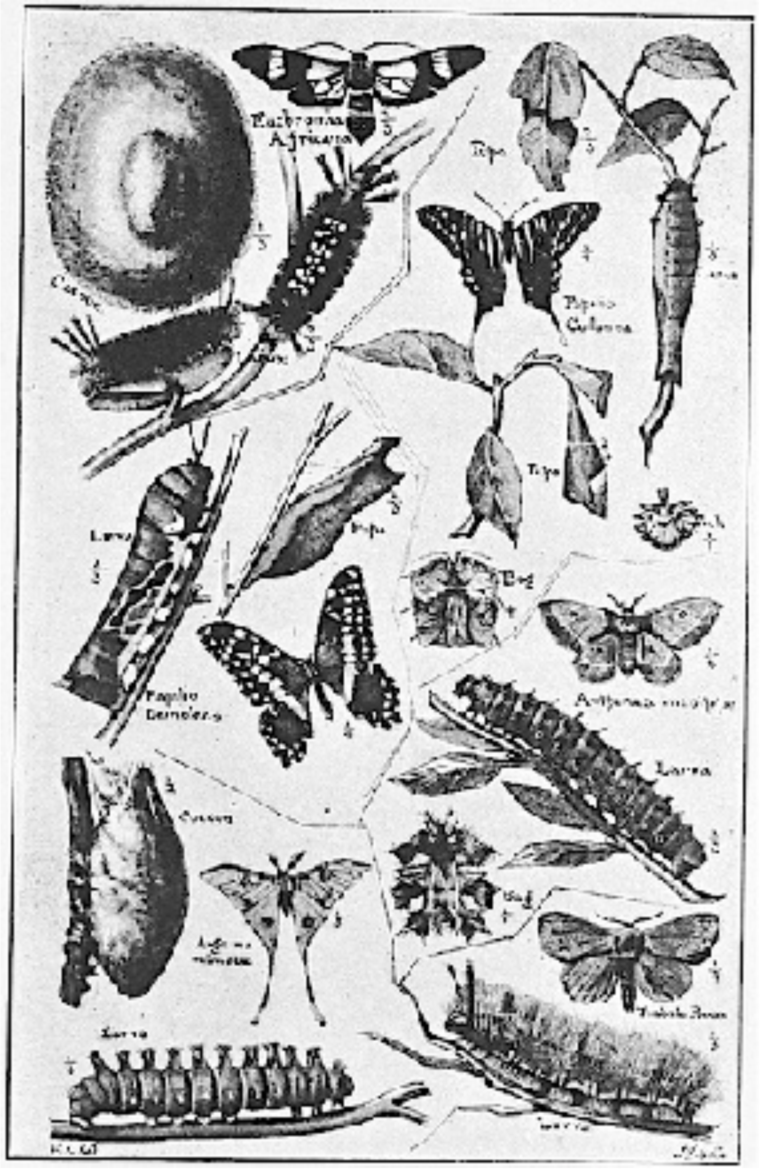
Endemic Risk Quadrants



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

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

Security from Inventory



Enumerate your apps.

Generate their dependency graphs.

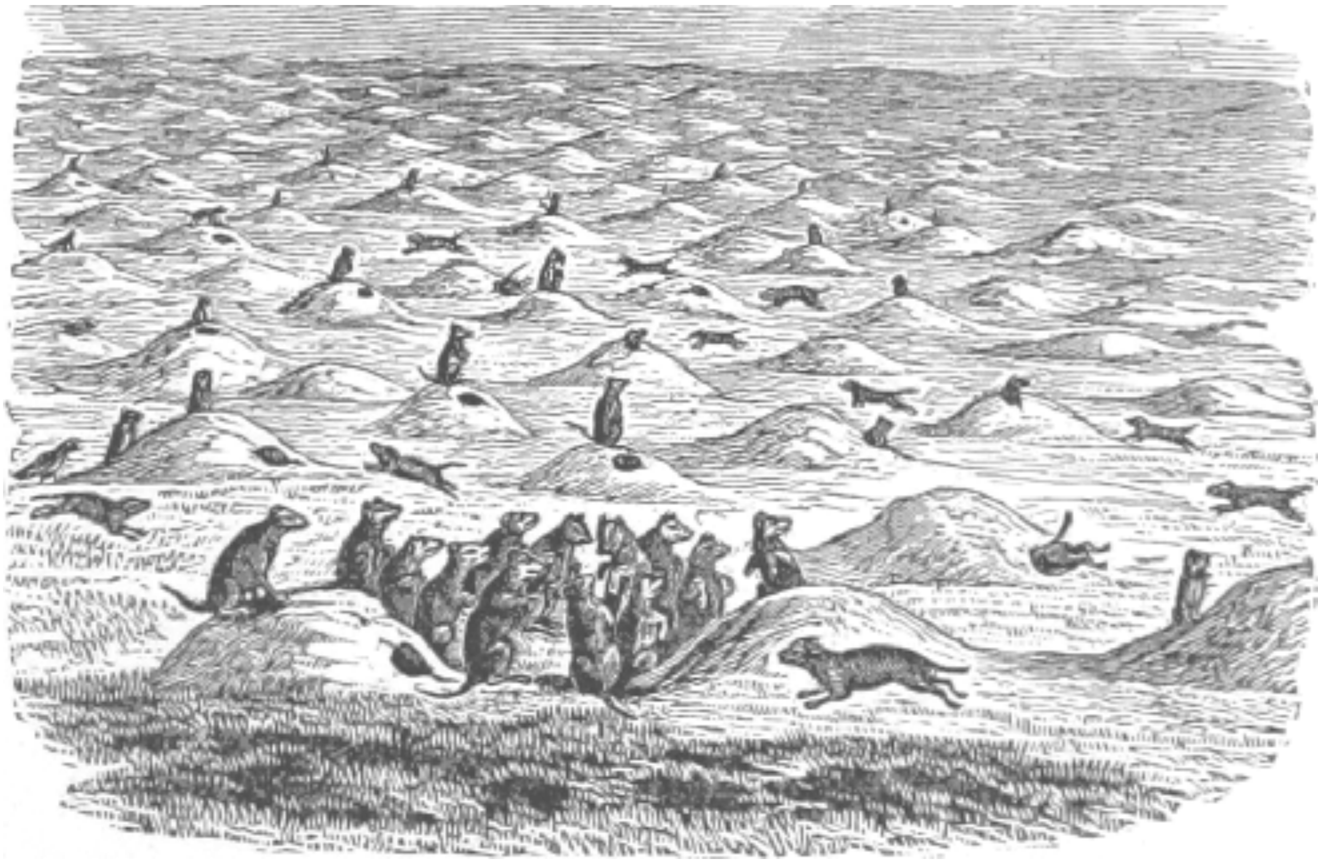
Identify ownership.

Security from Crowds

Provide reasonable threat models.

Report via issue trackers.

Automate reproduction steps.



Security from DevSecOps

Measure vuln discovery effort

Monitor risk for trends

Illuminate brittle design

DevSecCon | LONDON 19-20 OCT 2017

Thank You!

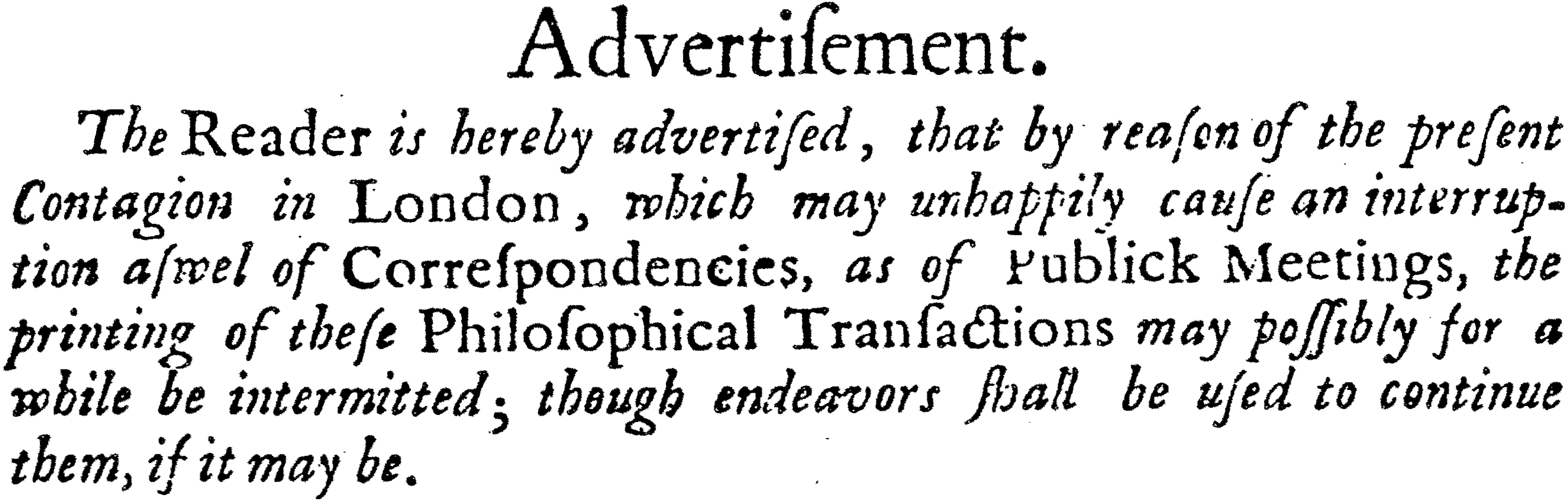
Join the conversation #DevSecCon

DevSecCon | LONDON 19-20 OCT 2017

Questions?

@CodexWebSecurum

Join the conversation #DevSecCon



Advertiſement.

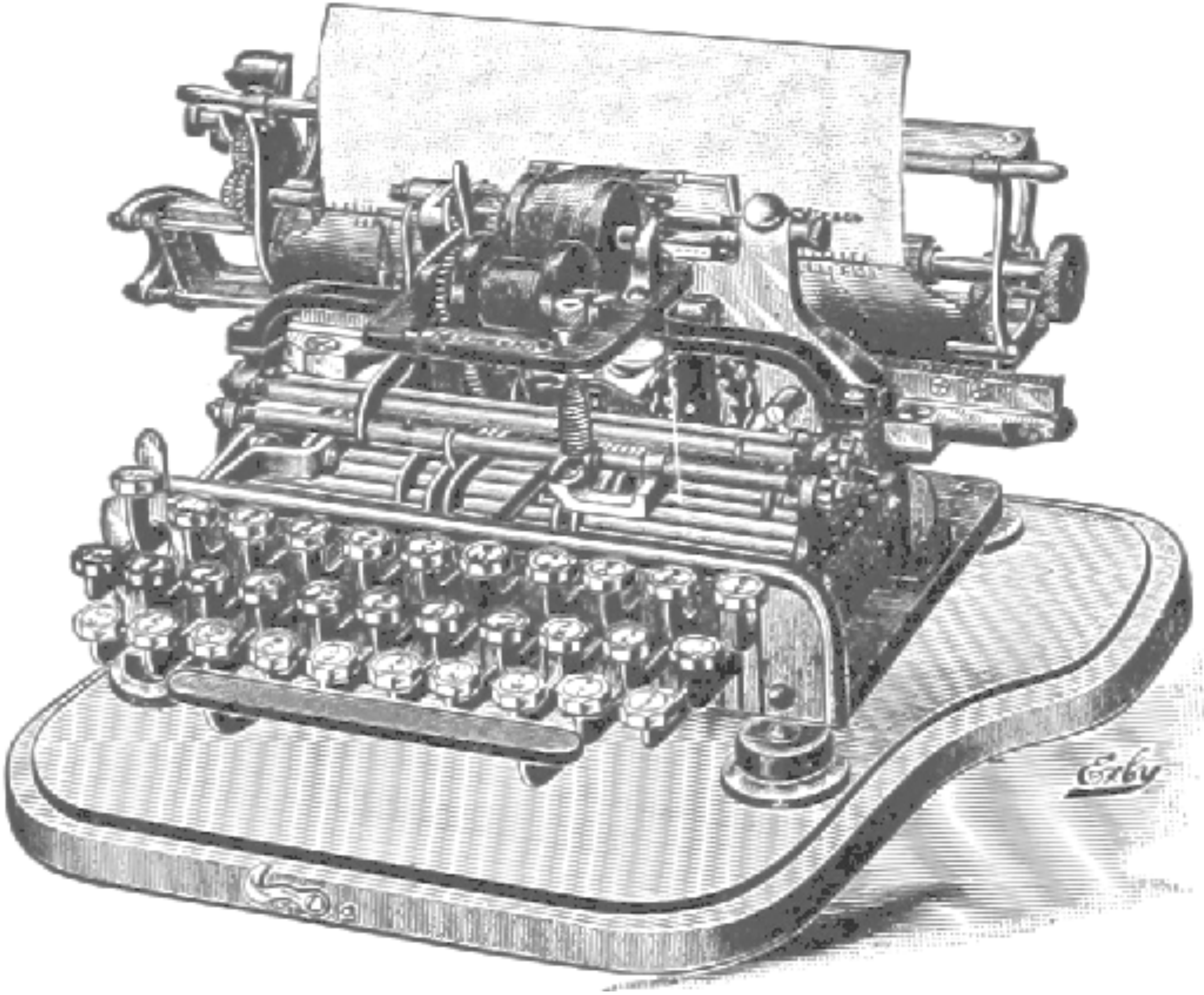
The Reader *is hereby advertiſed, that by reaſon of the preſent Contagion in* London*, which may unhappily cauſe an interruption aſwel of* Correſpondencies, *as of* Publick Meetings, *the printing of theſe* Philoſophical Tranſactions *may poſſibly for a while be intermitted; though endeavors ſhall be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

R —
  www.r-project.org

RStudio —
  www.rstudio.com

`data.table`

`ggplot`



A **cacophony** of hordes.

A **scrutiny** of crowds.