# Measuring & Maximizing Crowdsourced Vuln Discovery

Mike Shema
mike@cobalt.io

October 4, 2018

“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.”

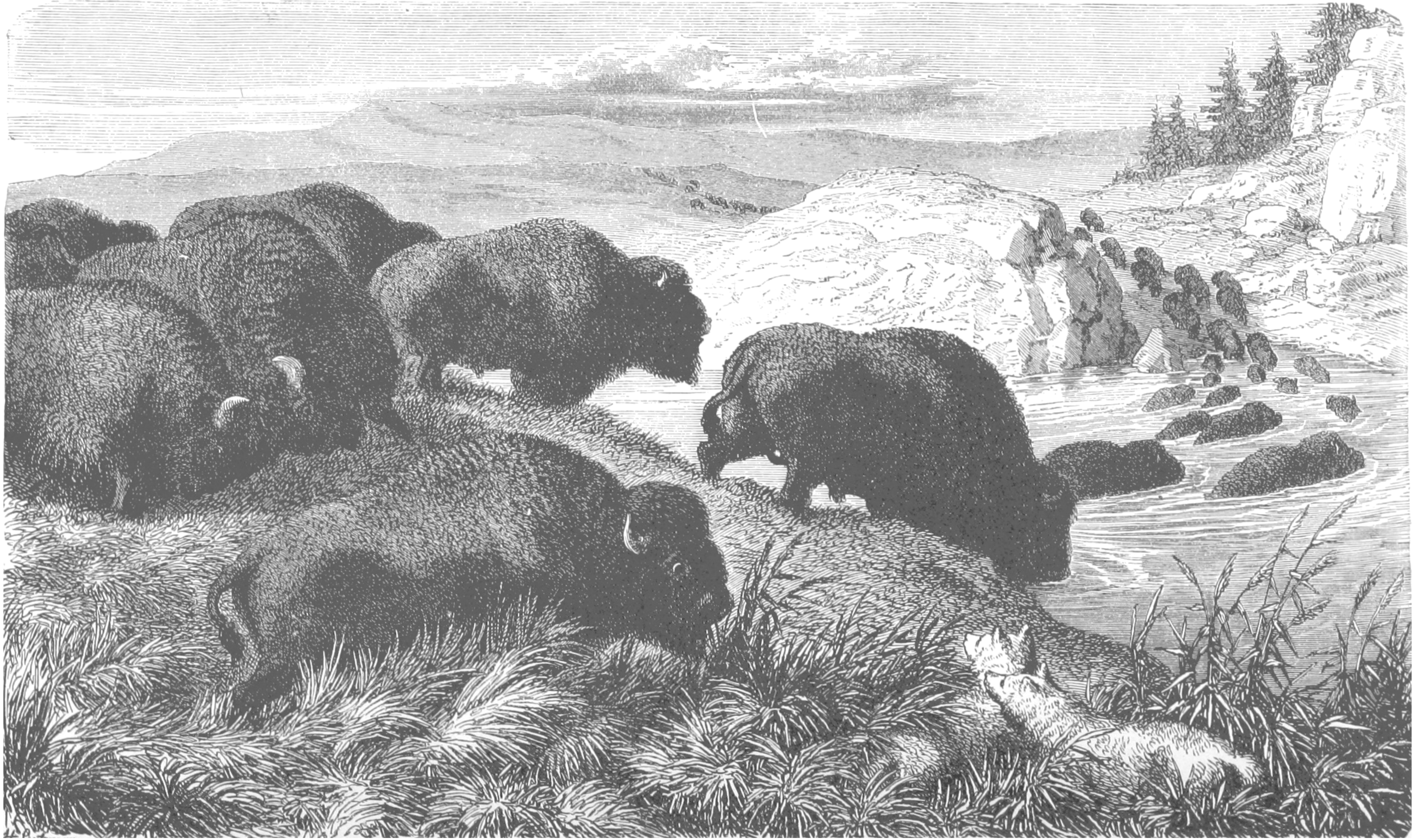
– Eli Wallach, *The Good, the Bad, and the Ugly*.

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

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

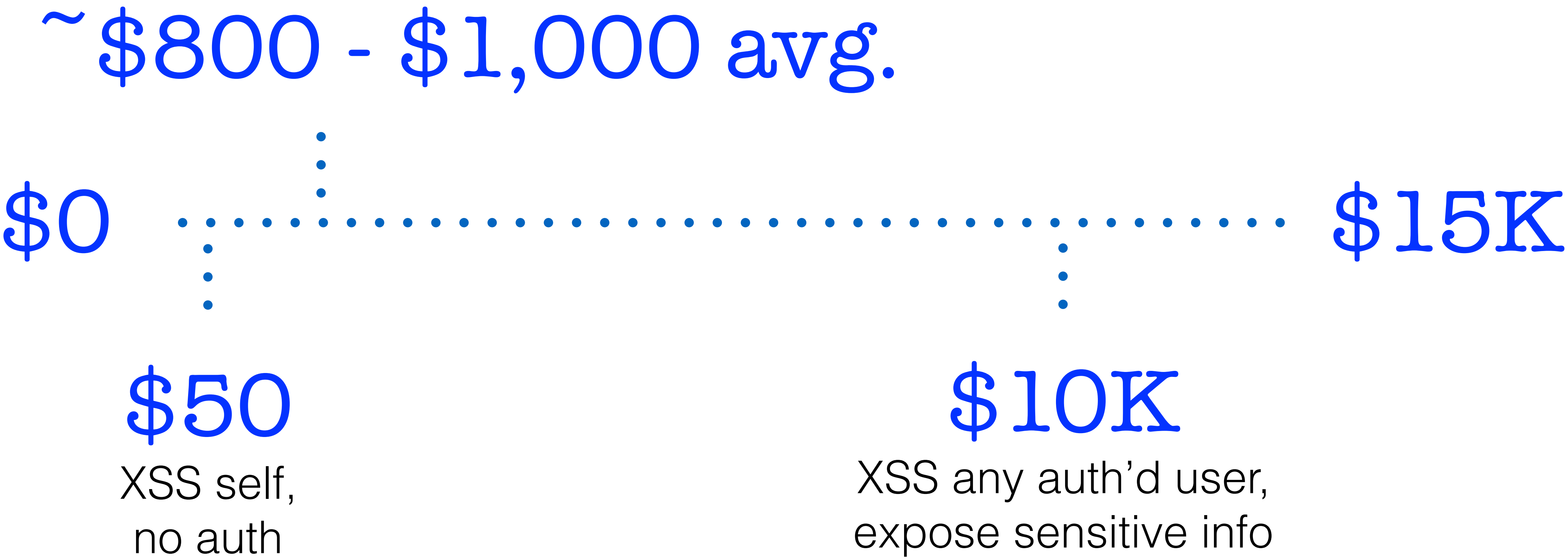
“What’s the **value** of finding vulns?”
— CSOs

“**When?**”
— Everyone



Vulns. Bounties. Crowds. Herds.

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



~$800 - $1,000 avg.

$0

$15K

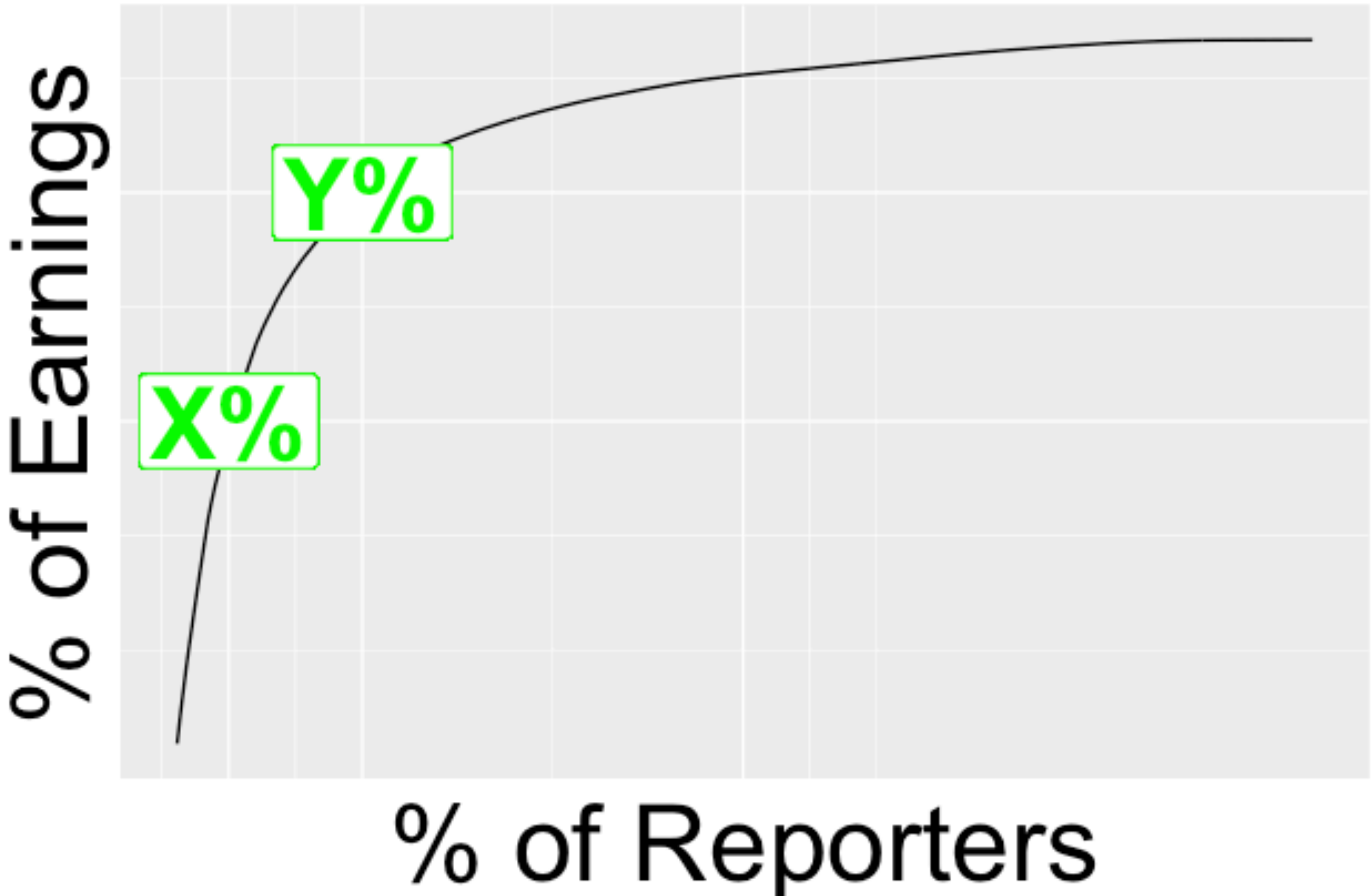
$50

XSS self,
no auth

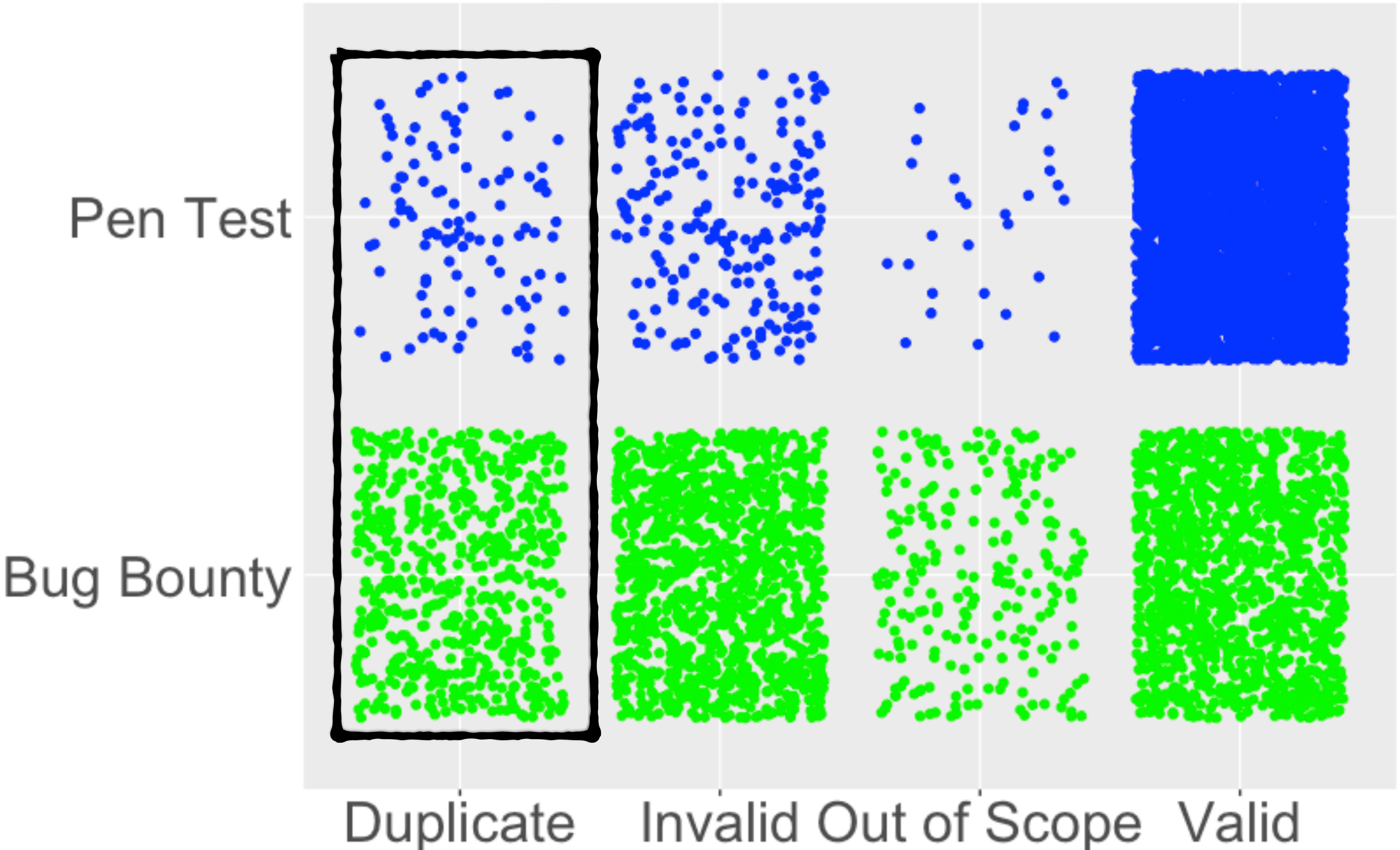
$10K

XSS any auth'd user,
expose sensitive info

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



# Acceptance State of Vulns



Noise increases cost of discovery and reduces efficiency.

# Build a Story (Cautiously)

Ask an interesting question.

Collect signals, beware silence.

Create metrics, beware tunnel vision.

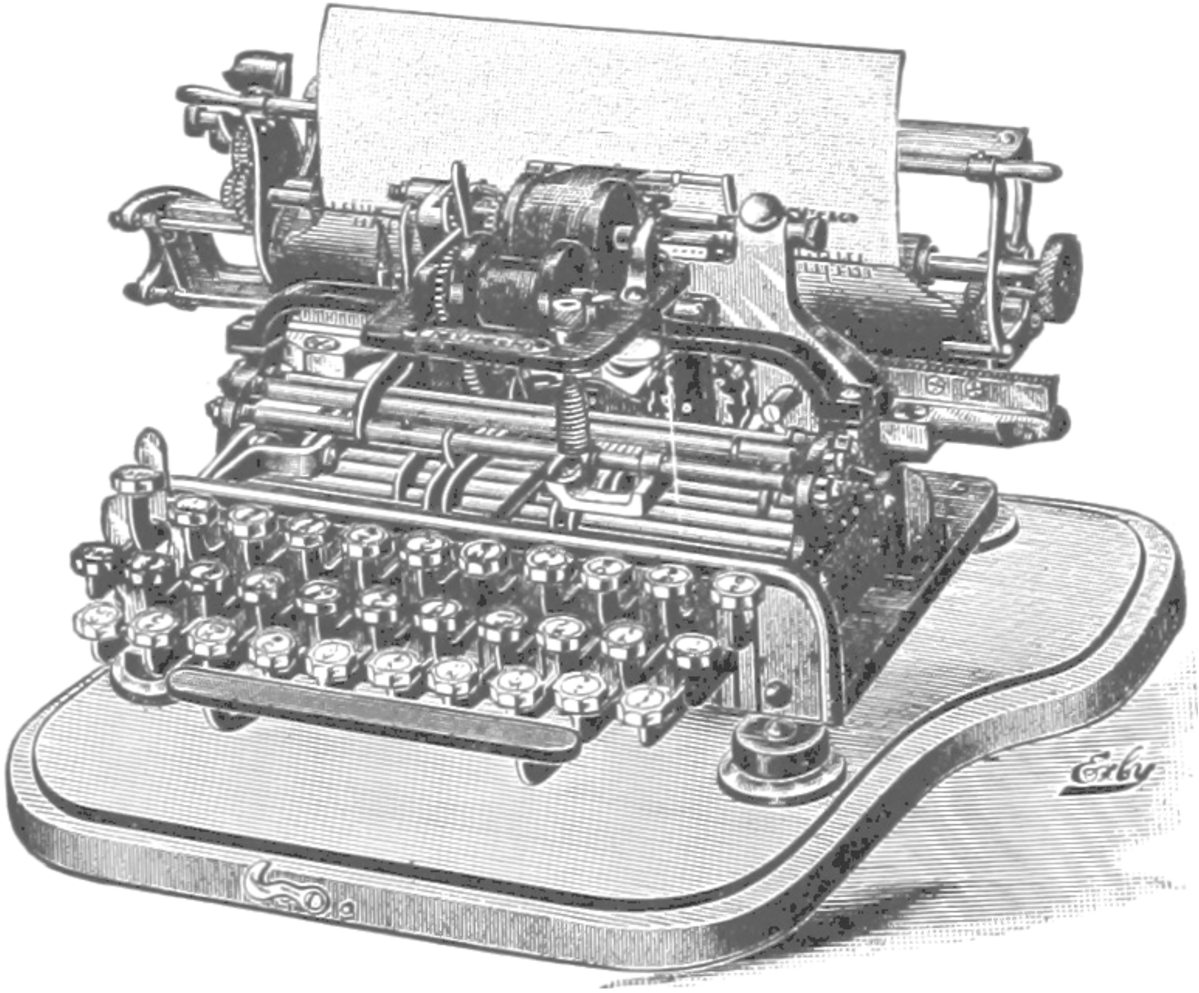
Create a story, beware myth.

R, www.r-project.org

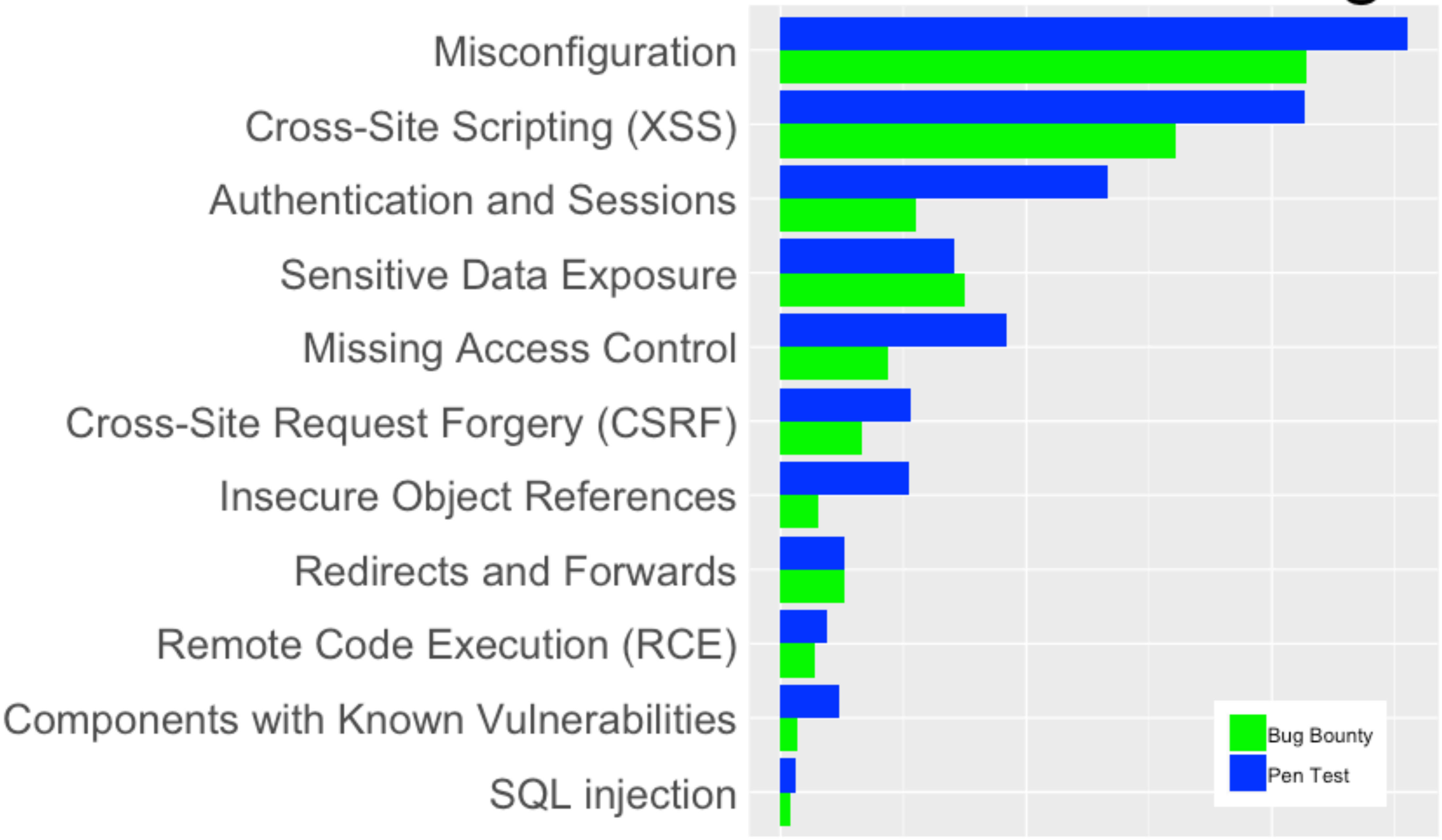
RStudio, www.rstudio.com

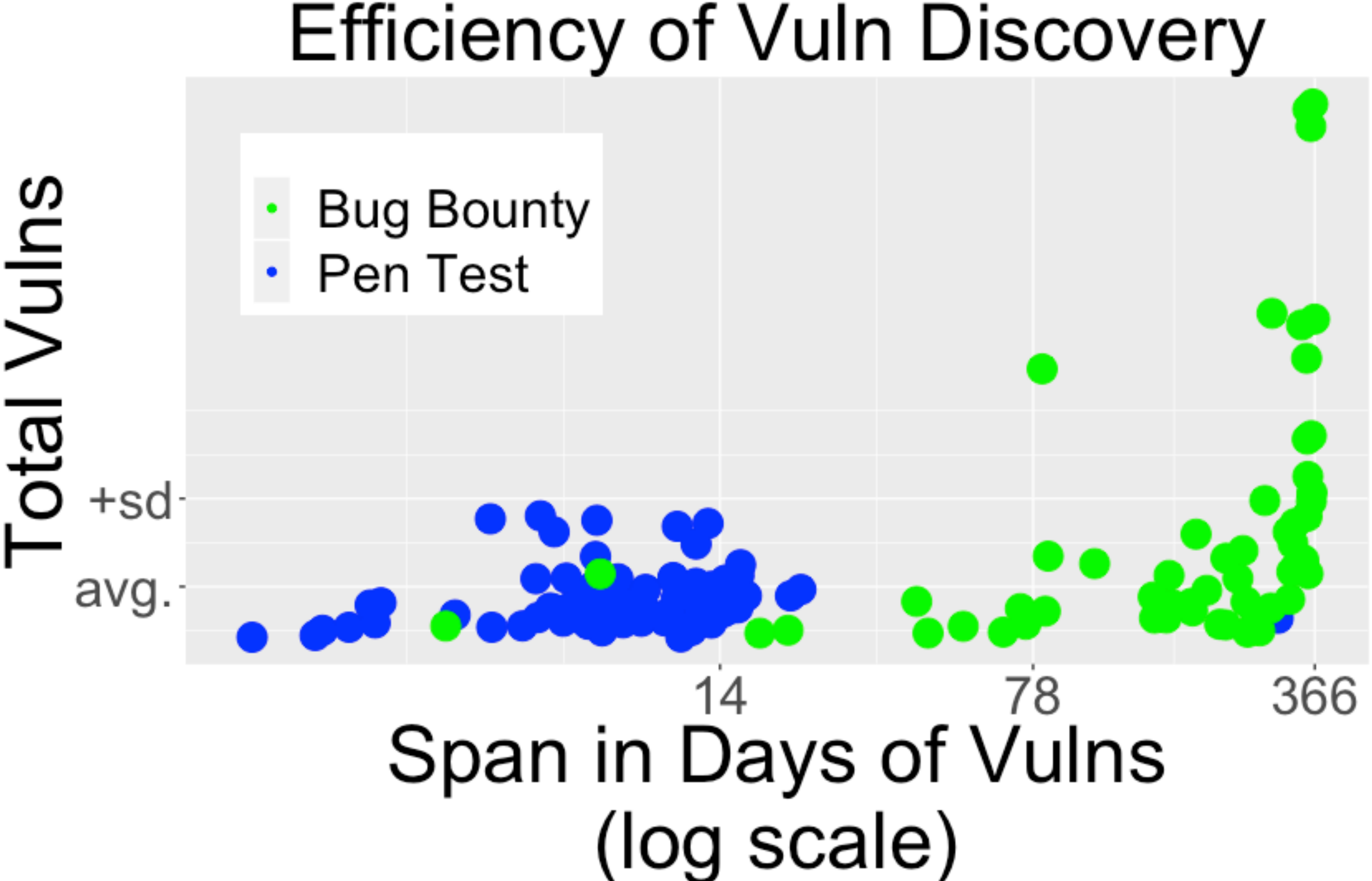
`data.table`

`ggplot2`

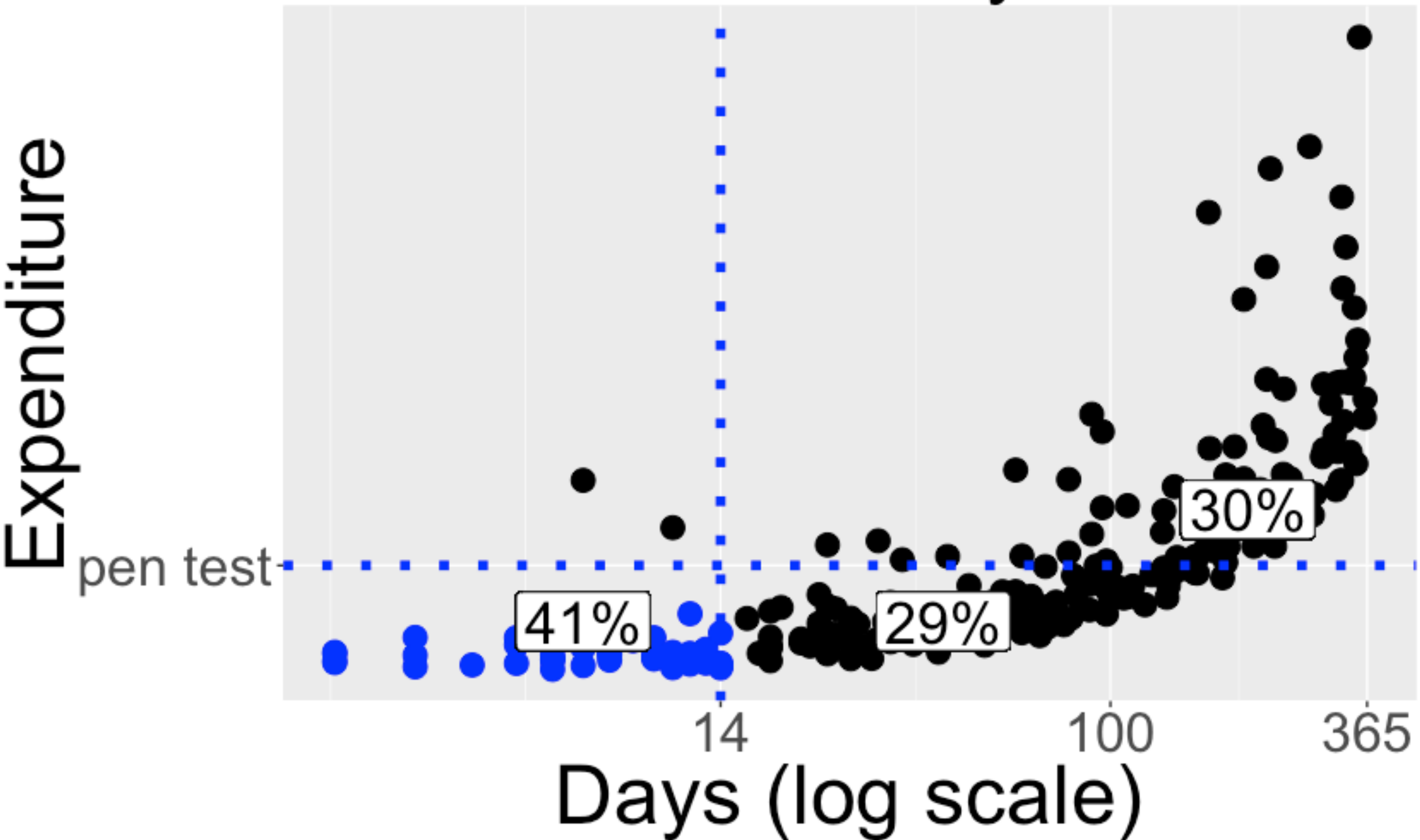


# Common Findings

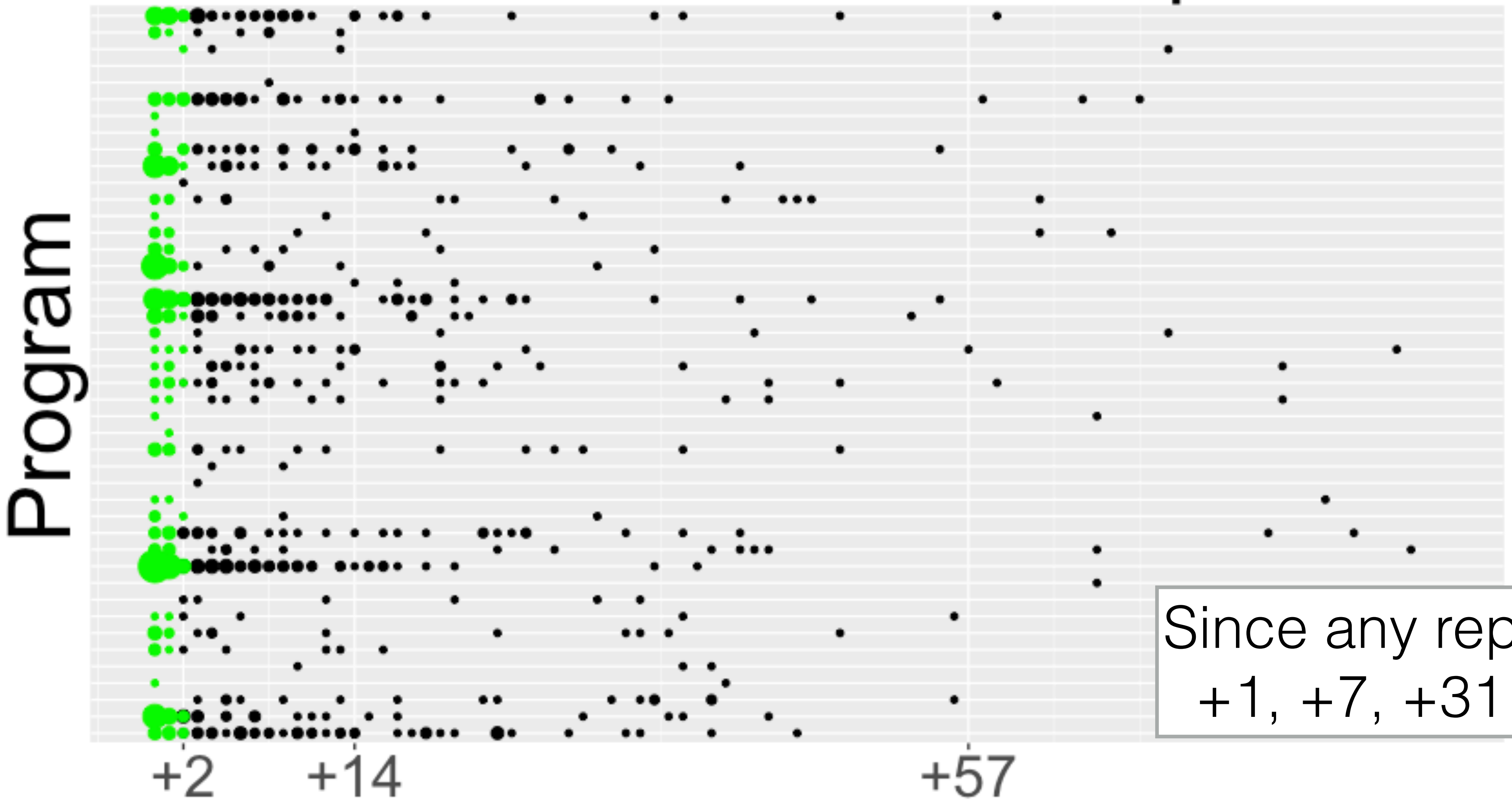



Efficiency of Vuln Discovery
Bug Bounty
Pen Test
Total Vulns
+sd
avg.
14
78
366
Span in Days of Vulns
(log scale)

# Vuln Discovery Cost



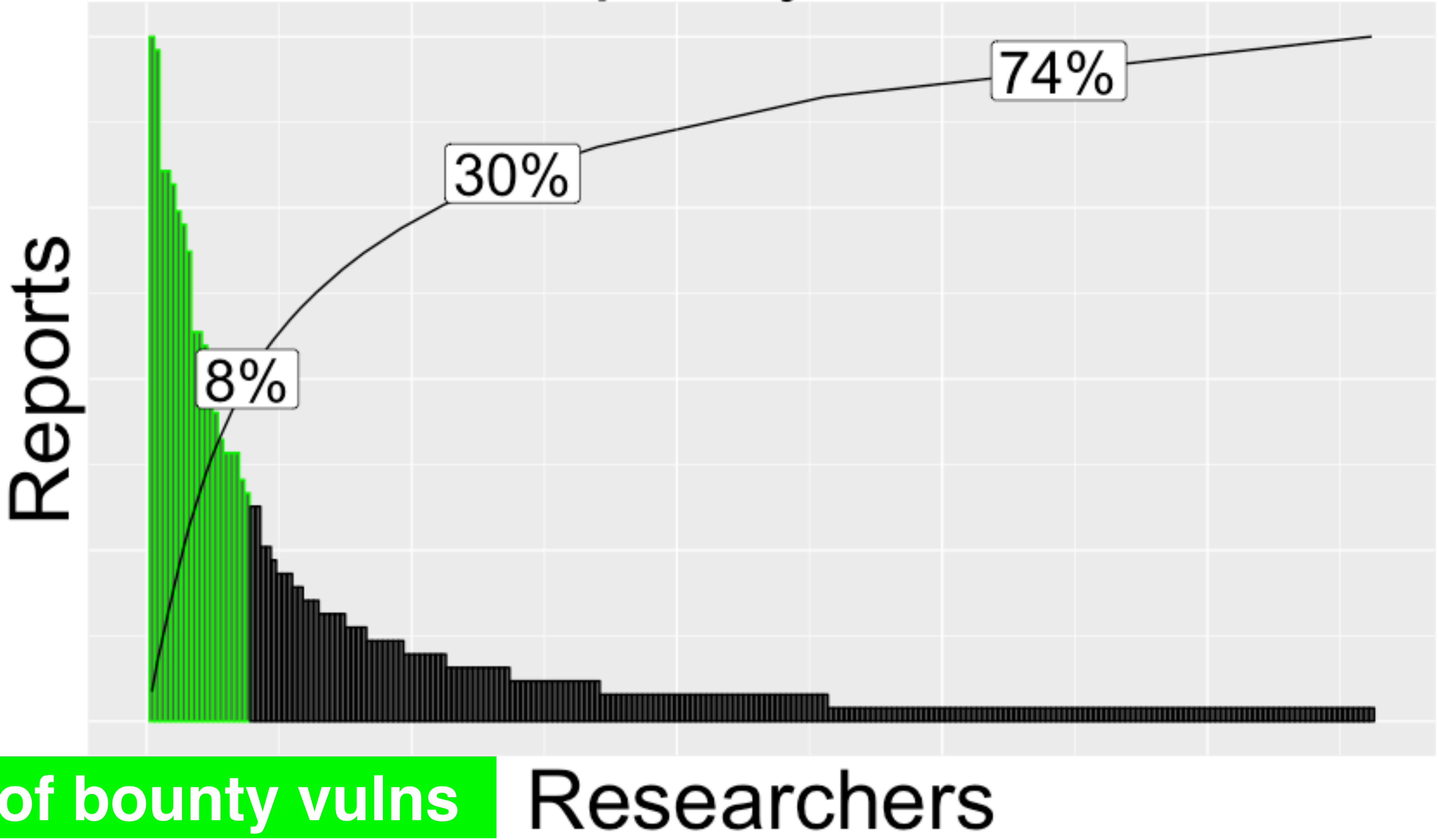
# Vuln Rate or Attention Span?



Days Since Previous Valid Report

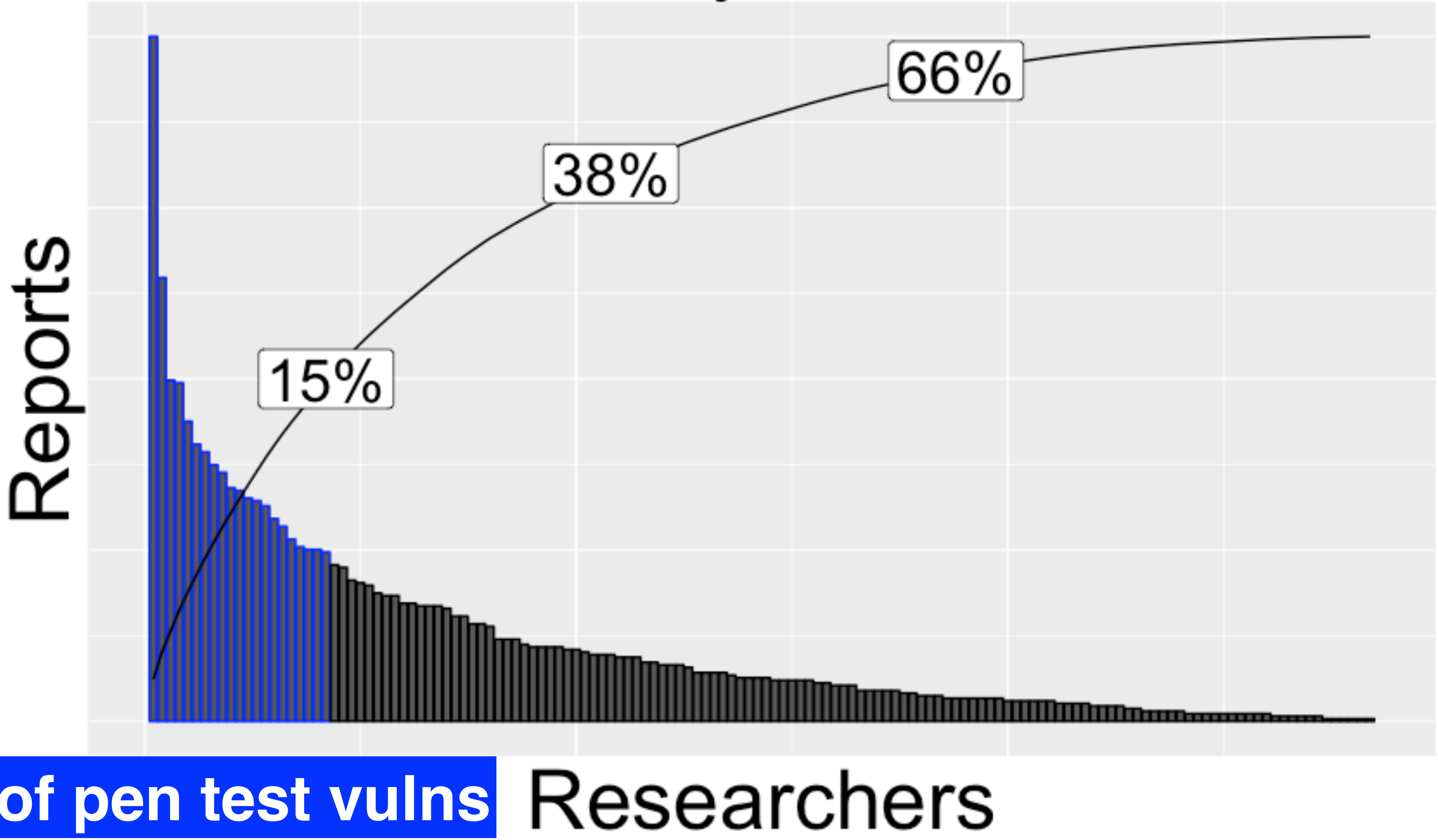
Since any report:
+1, +7, +31

# A Cacophony of Hordes



**50% of bounty vulns**

# A Scrutiny of Crowds

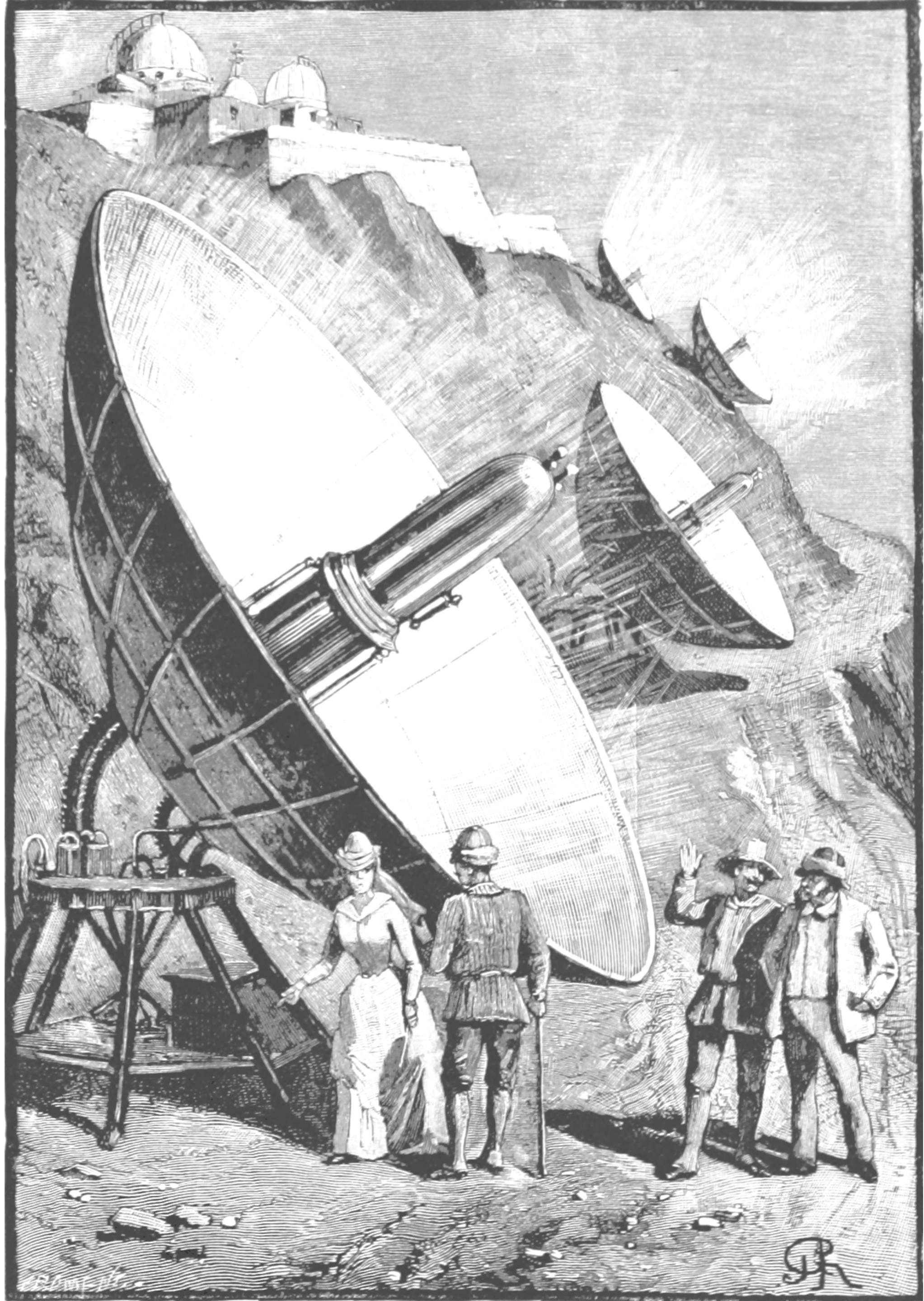


**50% of pen test vulns**

# Scanners

Overlaps and limitations in capabilities.

Fixed-cost, efficient, yet still require triage and maintenance.



# An Alliance of Appsec

Establish a baseline.

Refocus a noisy program.

Refine a stale program.

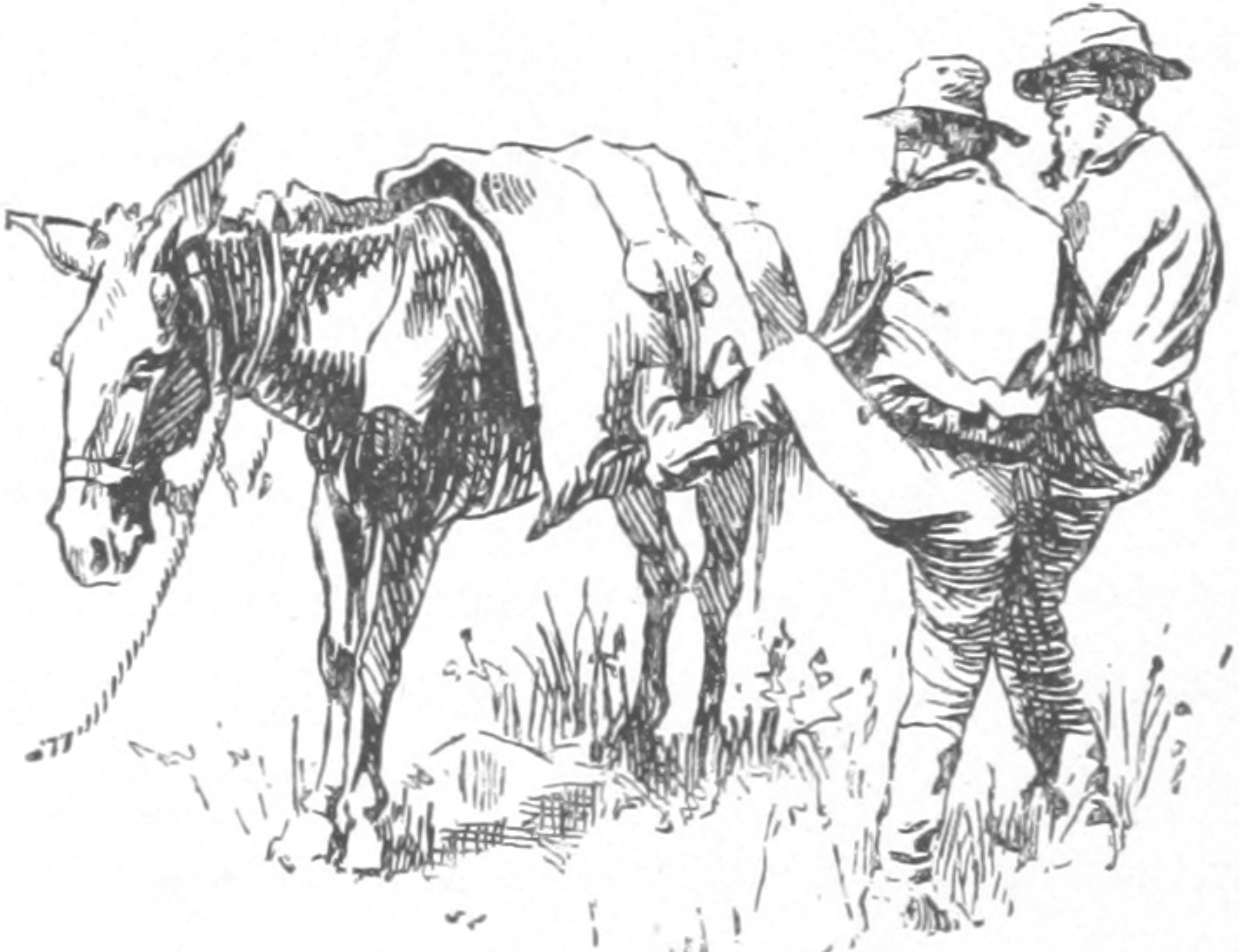
Identify effective bug finders.

Fix vulns, improve process.

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

# BugOps vs. DevOps

Chasing bugs isn’t a strategy.



## (shiftless)

Shift left isn’t merely finding vulns earlier.

Implement security controls earlier.

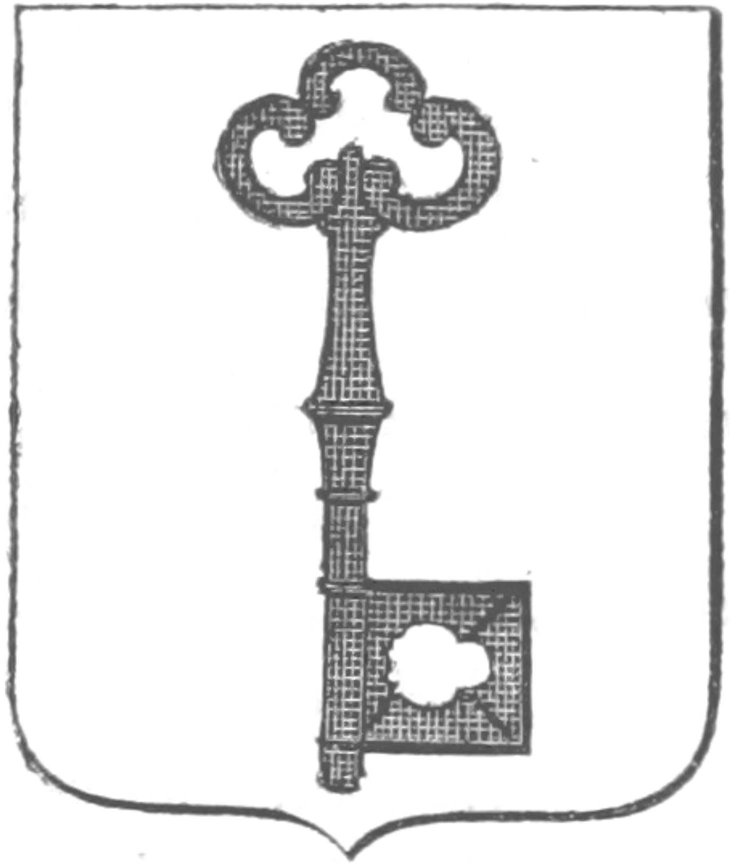
Design secure architectures earlier.

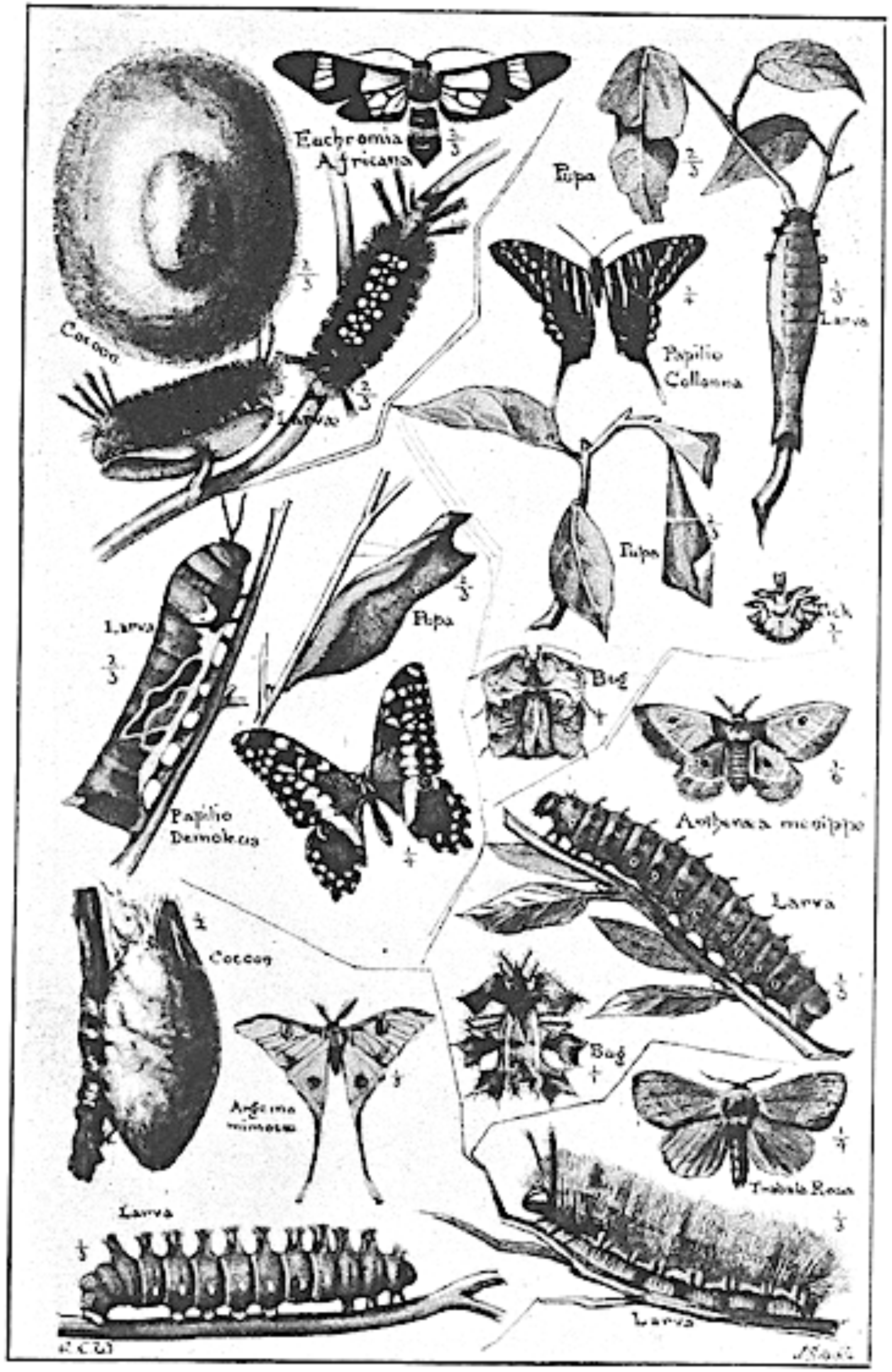
“You’re not using HTTPS.”

“Use HTTPS.”

“Seriously. Please use HTTPS.”

Let’s Encrypt.





# Always Basic

(never easy)

Enumerate apps.

Enumerate dependencies.

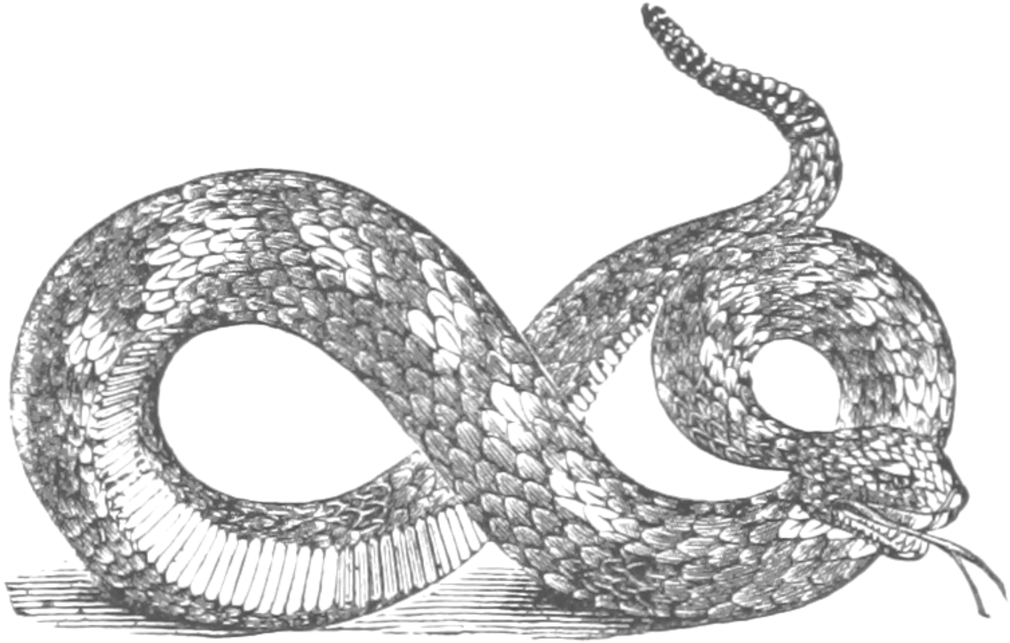
Identify ownership.

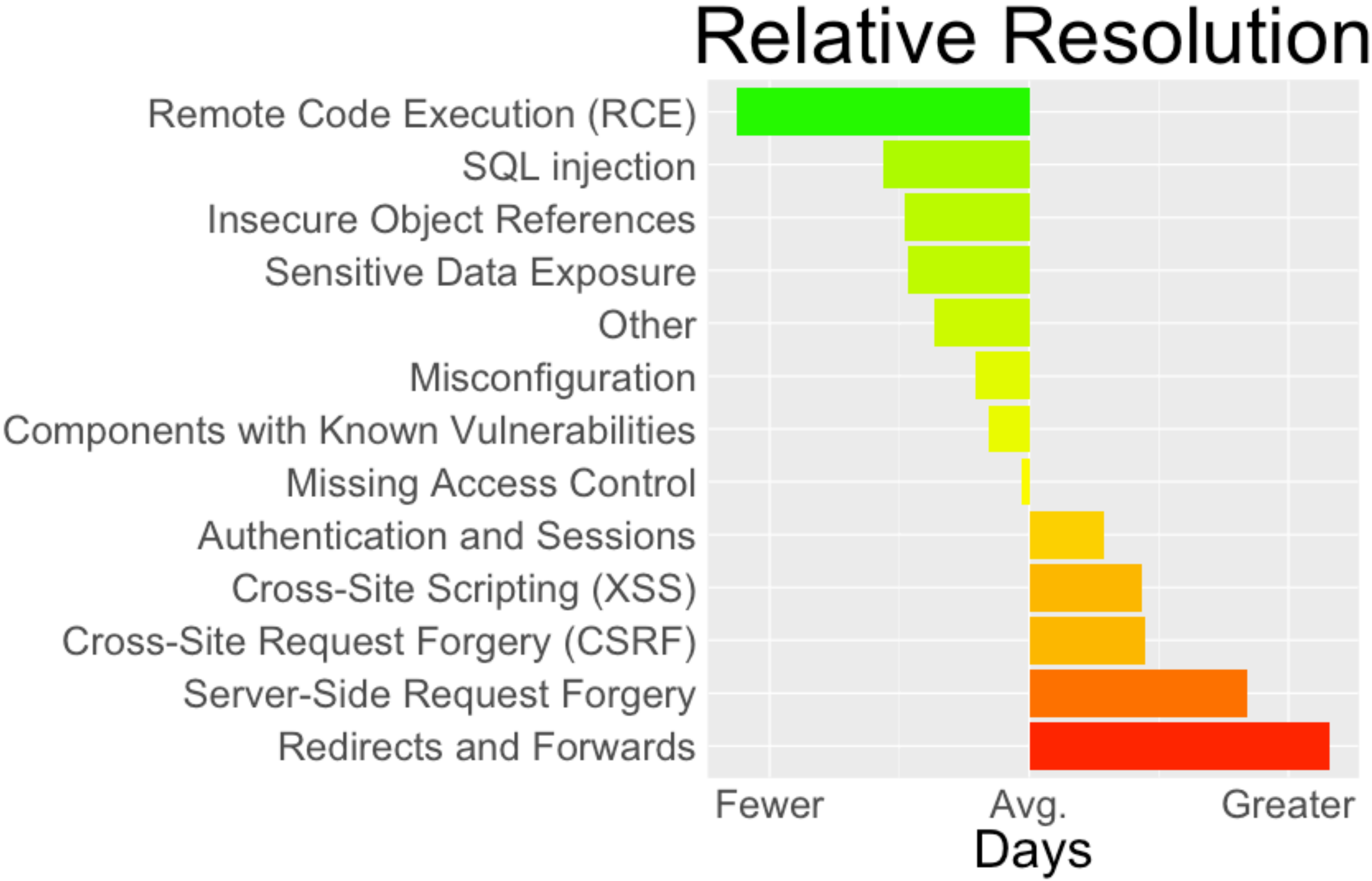
# Threat Modeling

DevOps exercise guided by security.

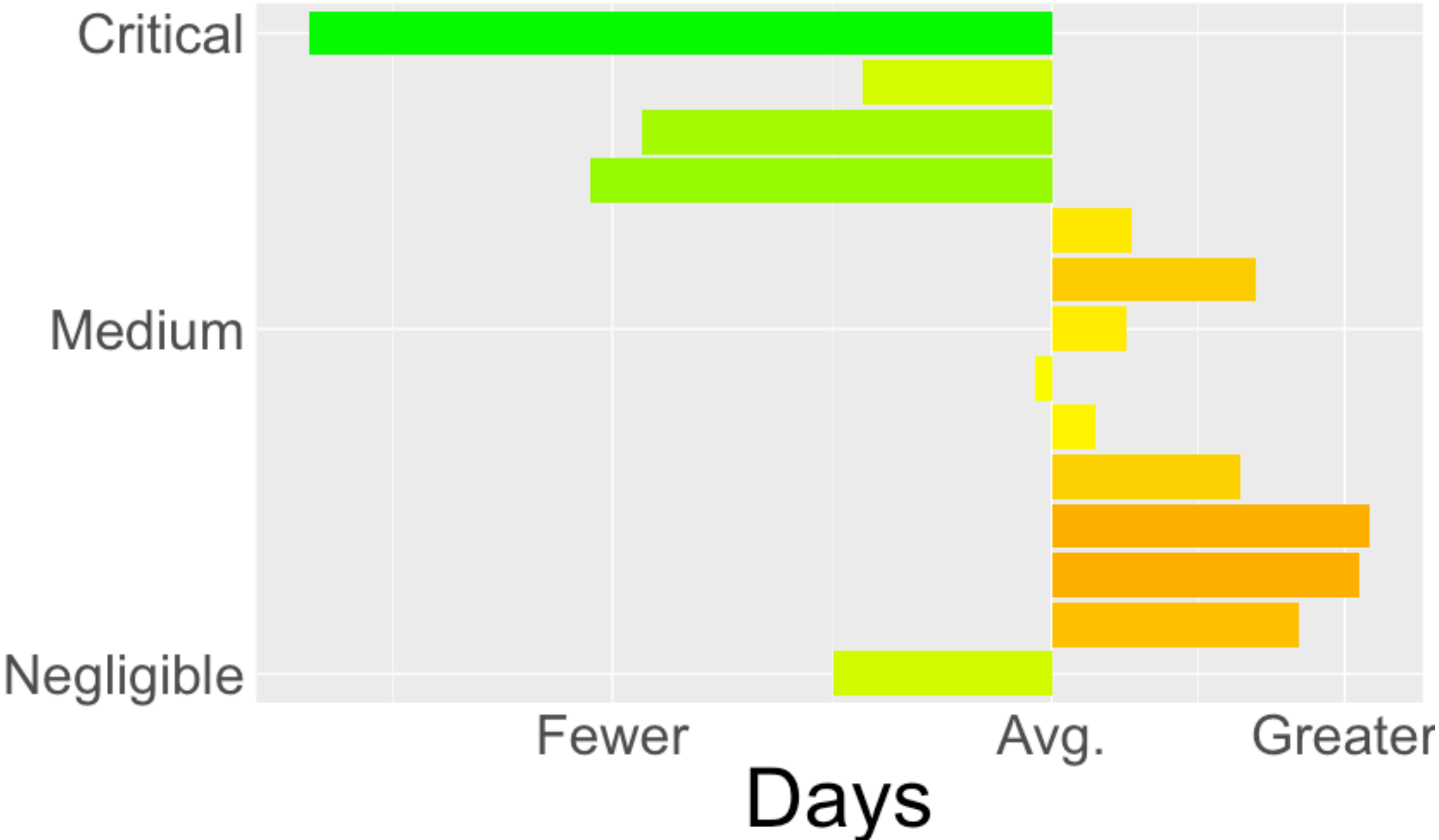
Influences design.

Informs implementation.




Relative Resolution
Remote Code Execution (RCE)
SQL injection
Insecure Object References
Sensitive Data Exposure
Other
Misconfiguration
Components with Known Vulnerabilities
Missing Access Control
Authentication and Sessions
Cross-Site Scripting (XSS)
Cross-Site Request Forgery (CSRF)
Server-Side Request Forgery
Redirects and Forwards
Fewer
Avg.
Greater
Days

# Relative Resolution of Risk

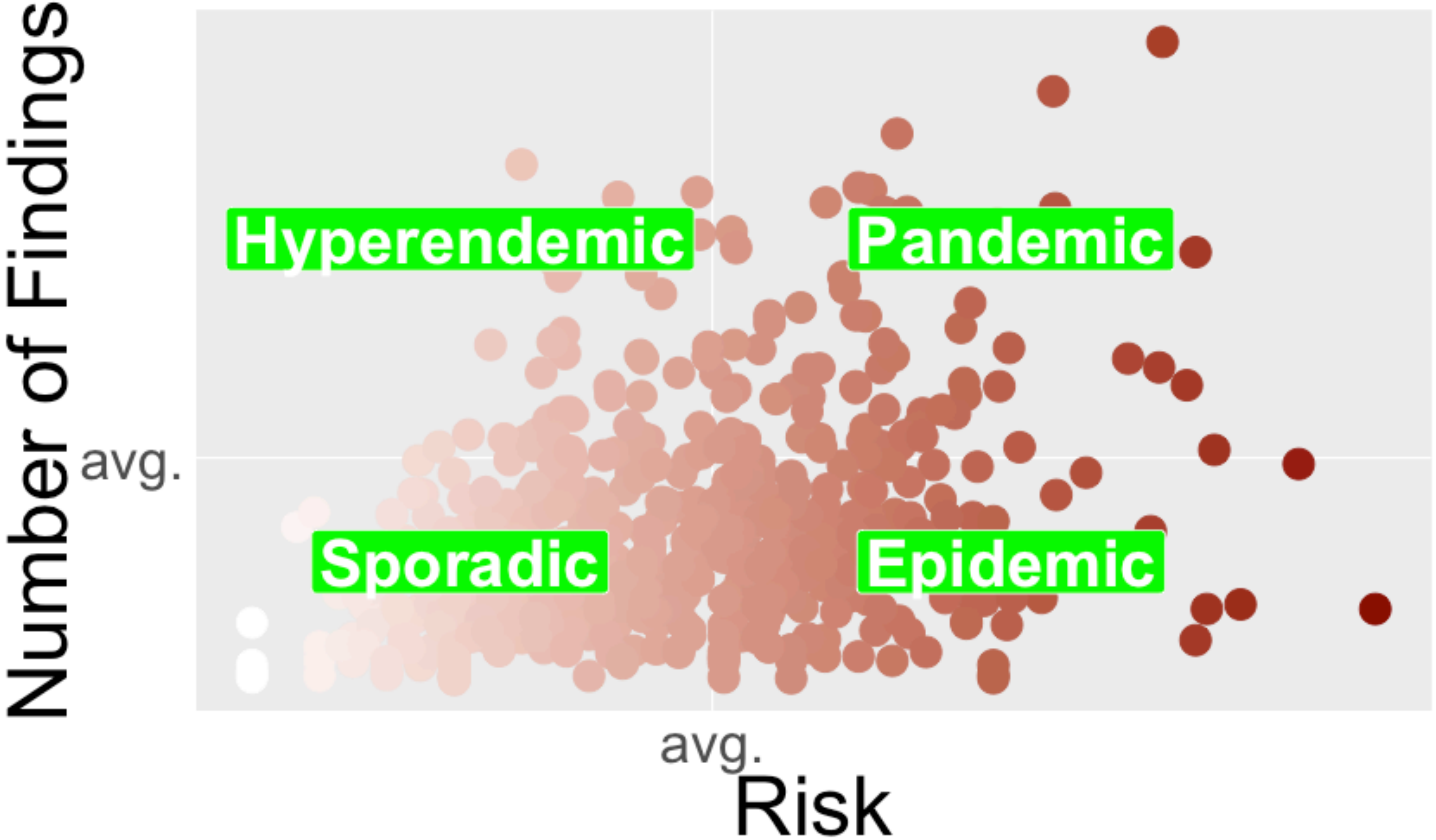


Maybe—

Most vulns are noise.

Many vulns aren’t worth fixing.

# Endemic Risk Quadrants



# “Spend Left”

Rebalance vuln discovery investments to favor the effort of discovering risk rather than the risk discovered.

When possible, invest in removing risk.

Who’s finding vulns in my app?

How often do they succeed?

What are they finding?

What’s the price paid for that effort?

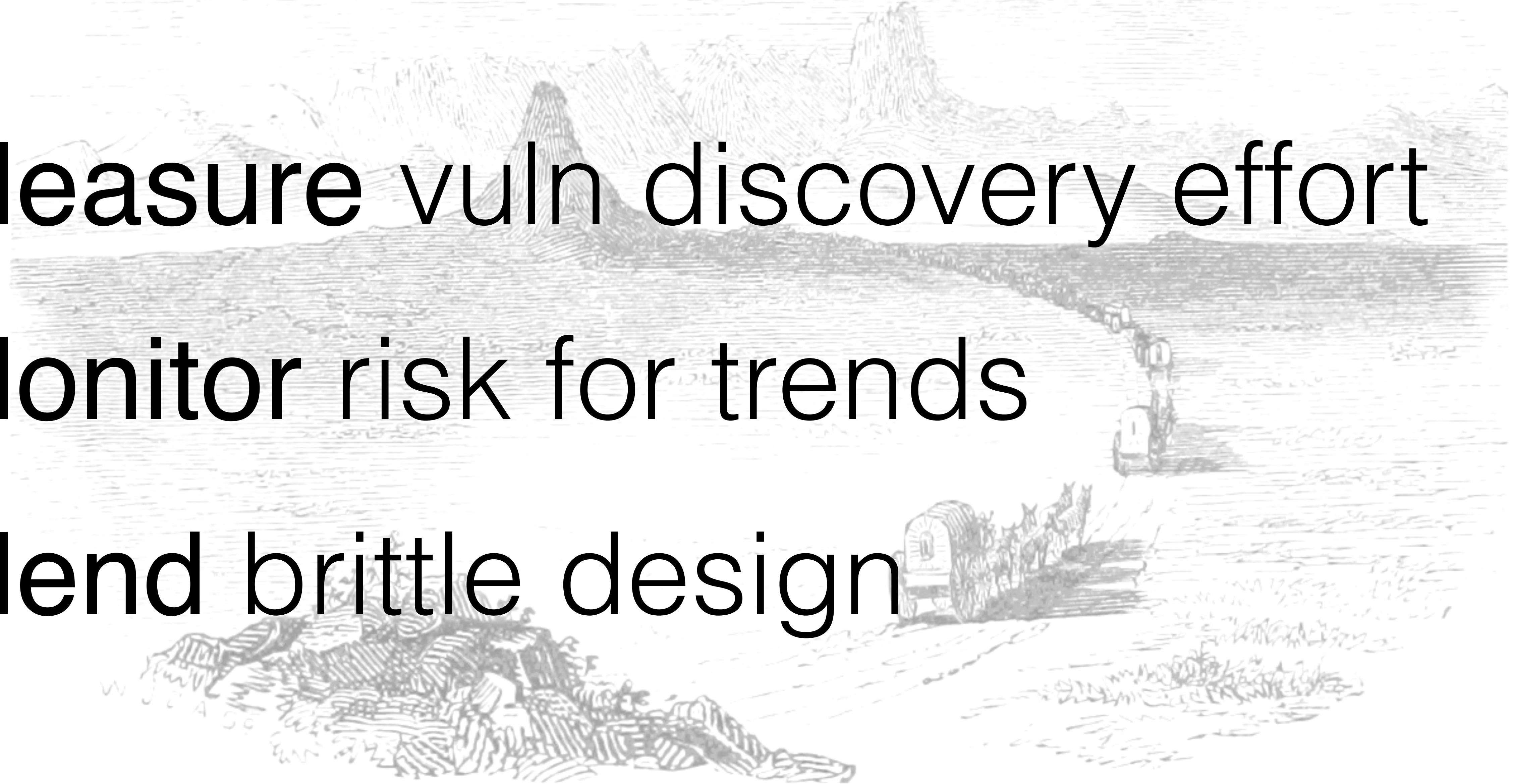
What’s the cost of [not] fixing the vulns?

What’s the risk that’s been reduced?

# Bounty prices as a proxy for DevSecOps, where price implies maturity.

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

# Dev[Sec]Ops



Measure vuln discovery effort

Monitor risk for trends

Mend brittle design

# Thank You!

cobalt.io

# Questions?

@CodexWebSecurum

www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

www.owasp.org/index.php/Category:Threat_Modeling

github.com/bugcrowd/vulnerability-rating-taxonomy

www.iso.org/standard/45170.html

www.iso.org/standard/53231.html

www.r-project.org

github.com/Rdatatable/data.table/wiki

ggplot2.tidyverse.org