RSA®Conference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: HT-F03

The Etiology of Vulnerability Exploitation

Jay Jacobs

Data Scientist
Cyentia Institute
@jayjacobs

Michael Roytman

Chief Data Scientist
Kenna Security
@mroytman

Today’s Journey…

- Describing the Vulnerability Landscape

- Measuring the Effectiveness of Vulnerability Remedation

- What contributes to exploitation?

Data Sources

NVD

CVSS

CPE™
common platform enumeration

CWE™

REVERSING™
LABS

Kenna
Know Your Risk

CANVAS

Secureworks®

EXPLOIT
DATABASE

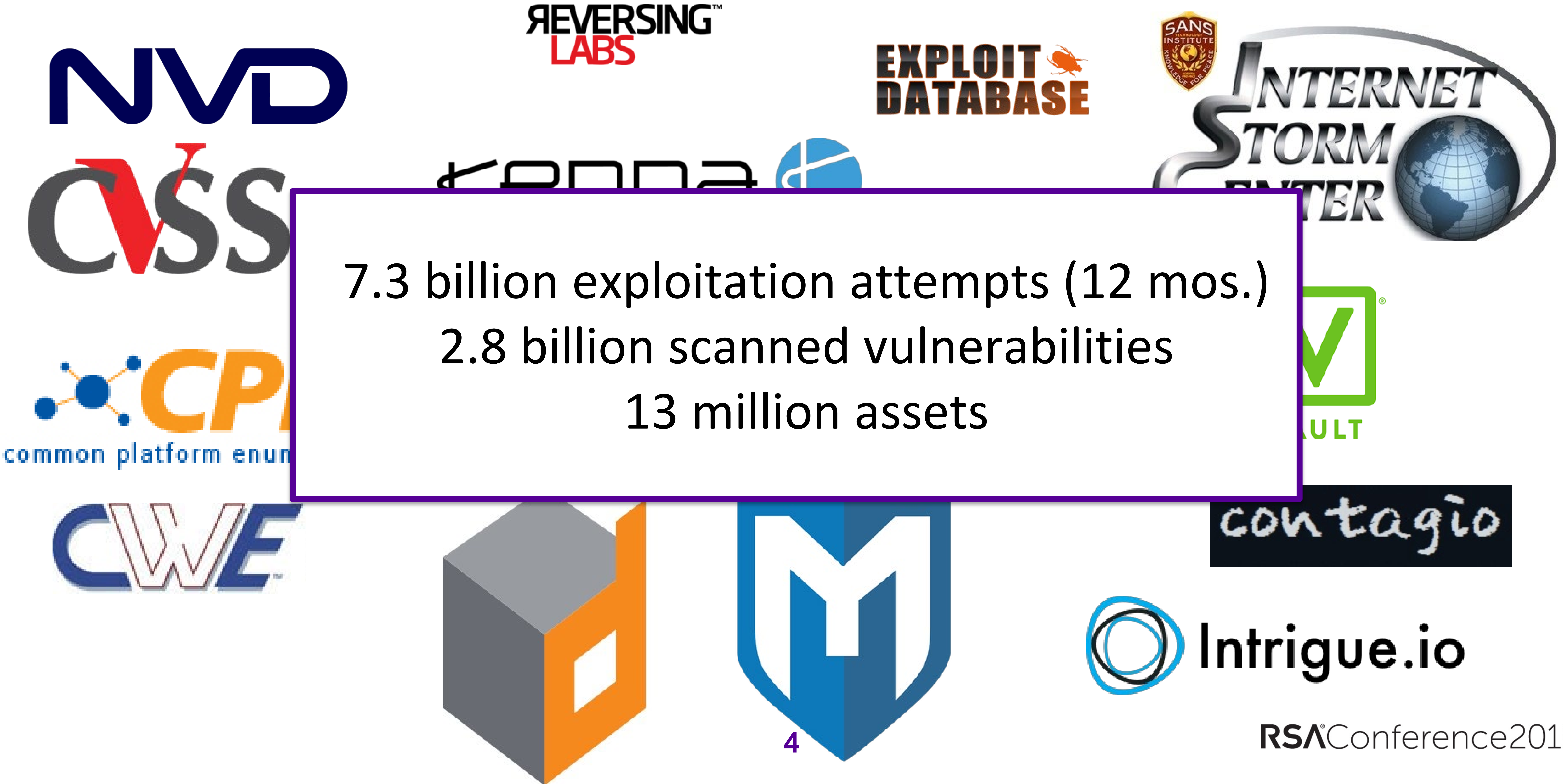
SANS INSTITUTE
INTERNET
STORM
CENTER

ALIEN VAULT®

contagio

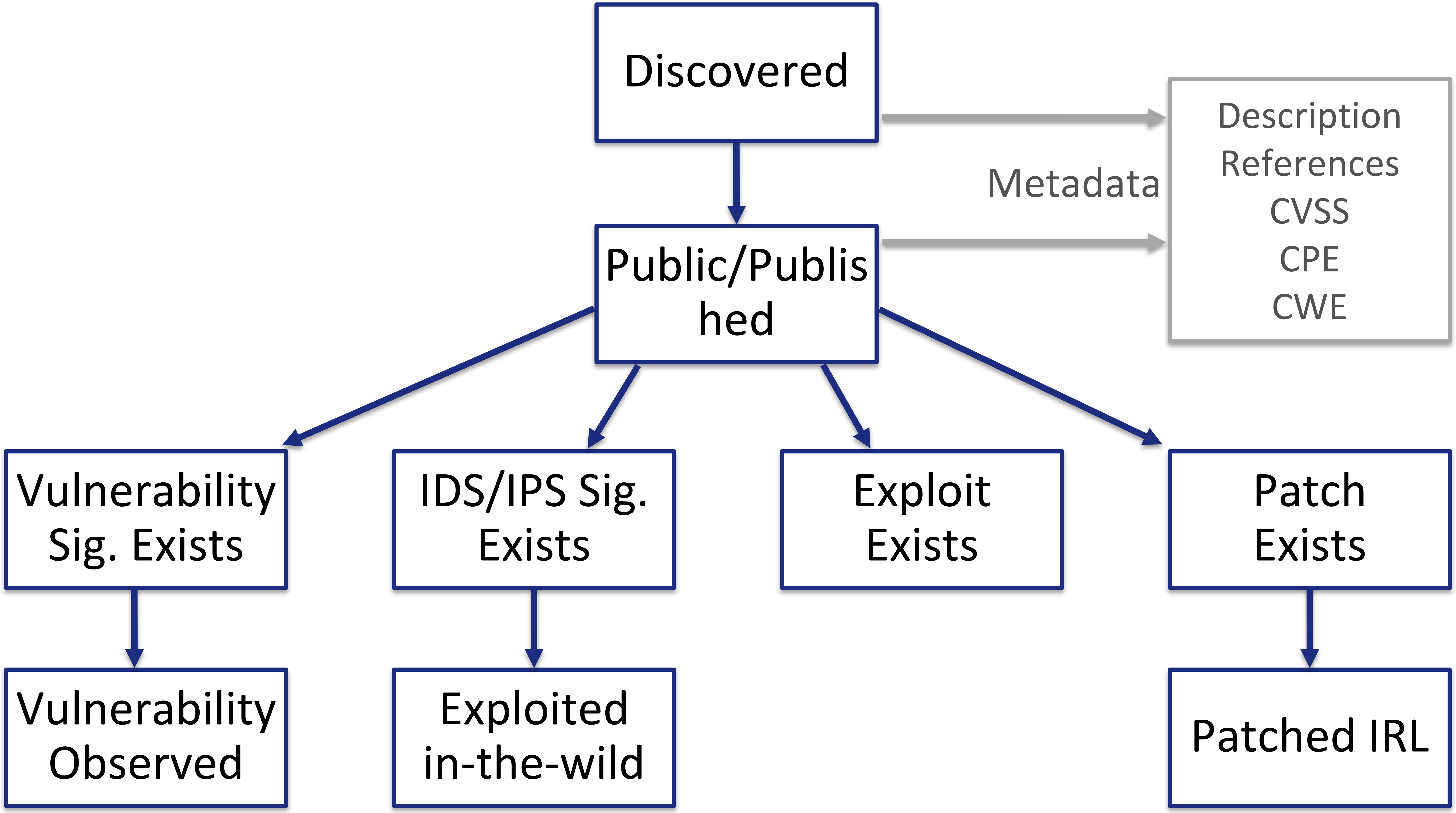
Intrigue.io

Data Sources

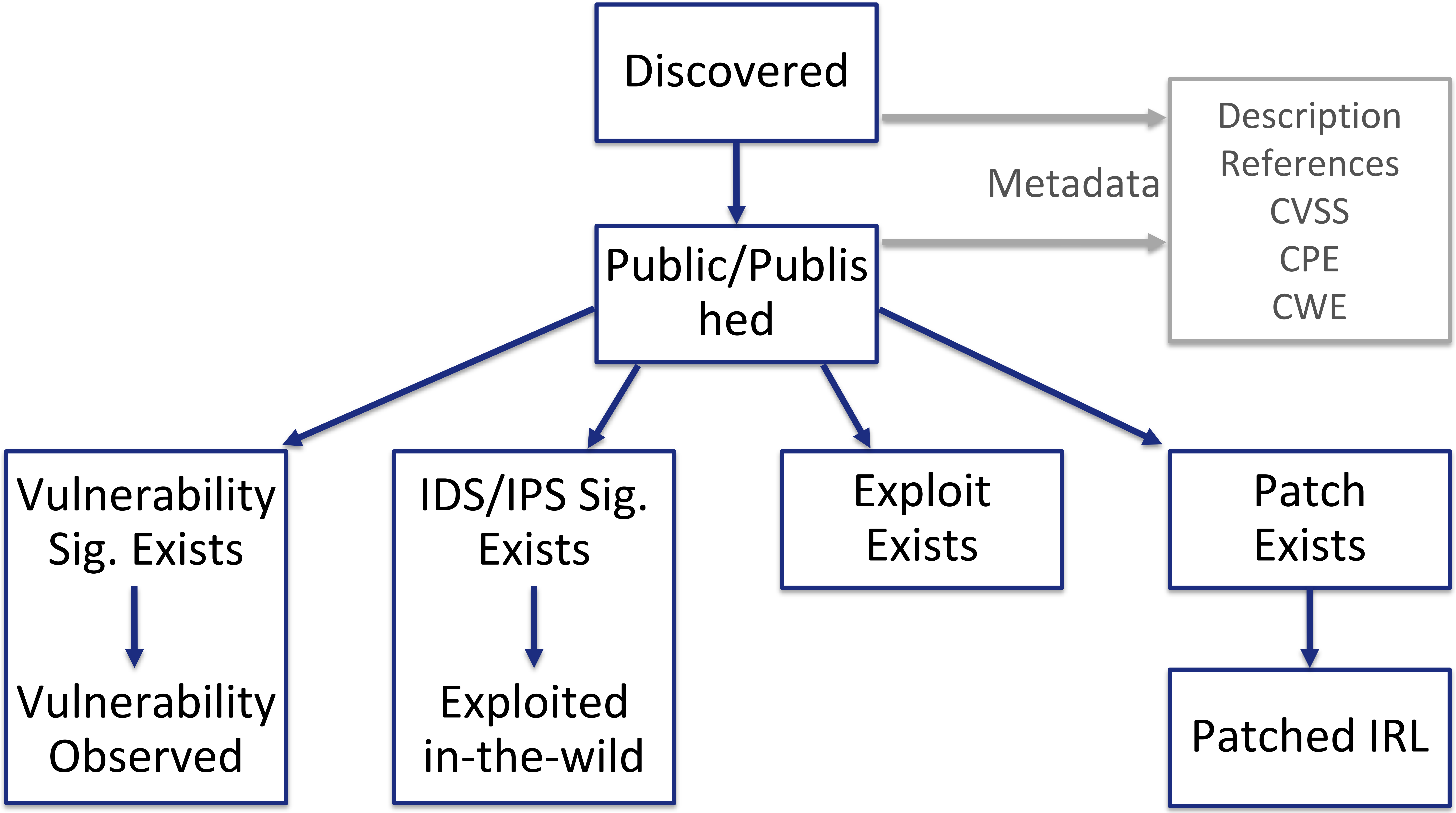


7.3 billion exploitation attempts (12 mos.)
2.8 billion scanned vulnerabilities
13 million assets

Simplified View of Vulnerabilities



Simplified View of Vulnerabilities



Discovered

Public/Published

Metadata

Description
References
CVSS
CPE
CWE

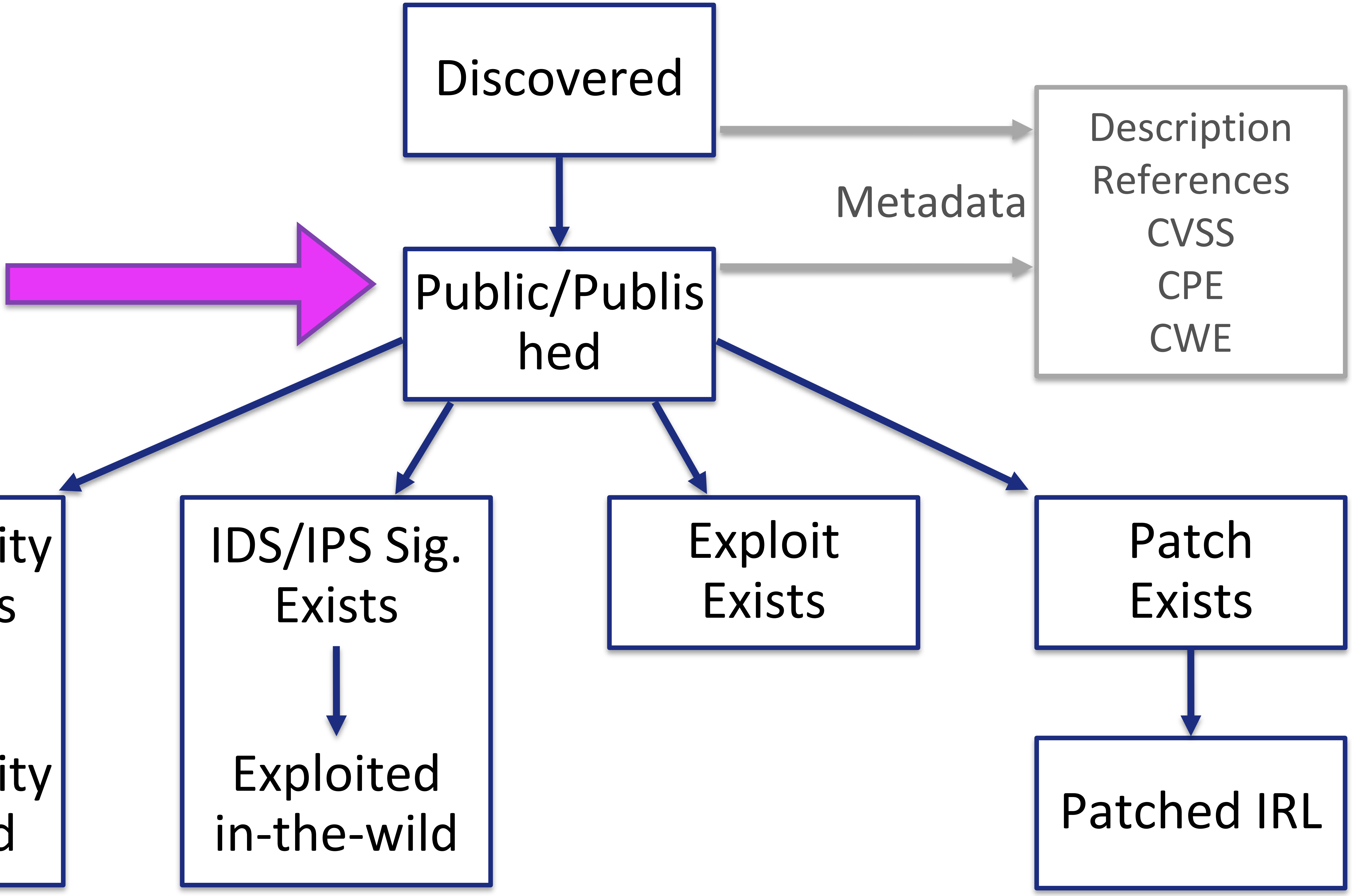
Vulnerability Sig. Exists → Vulnerability Observed

IDS/IPS Sig. Exists → Exploited in-the-wild

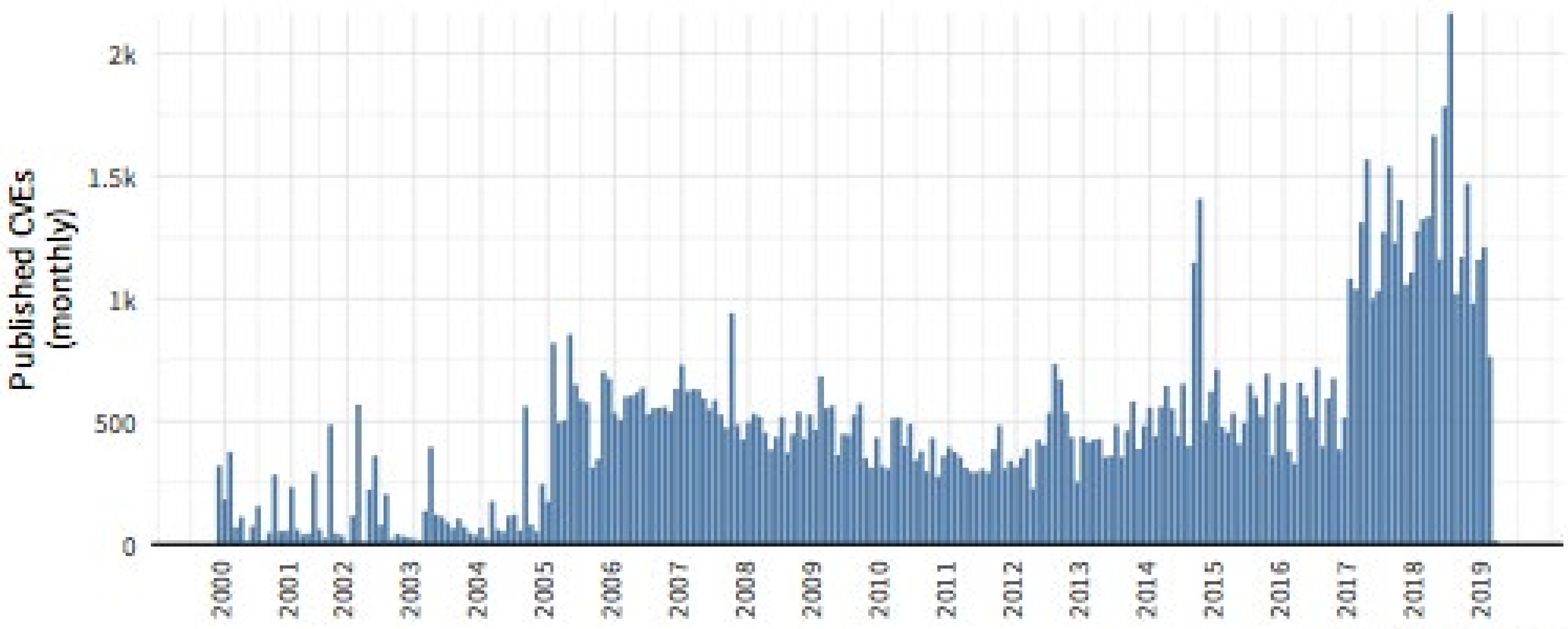
Exploit Exists

Patch Exists → Patched IRL

Simplified View of Vulnerabilities



The World of CVEs



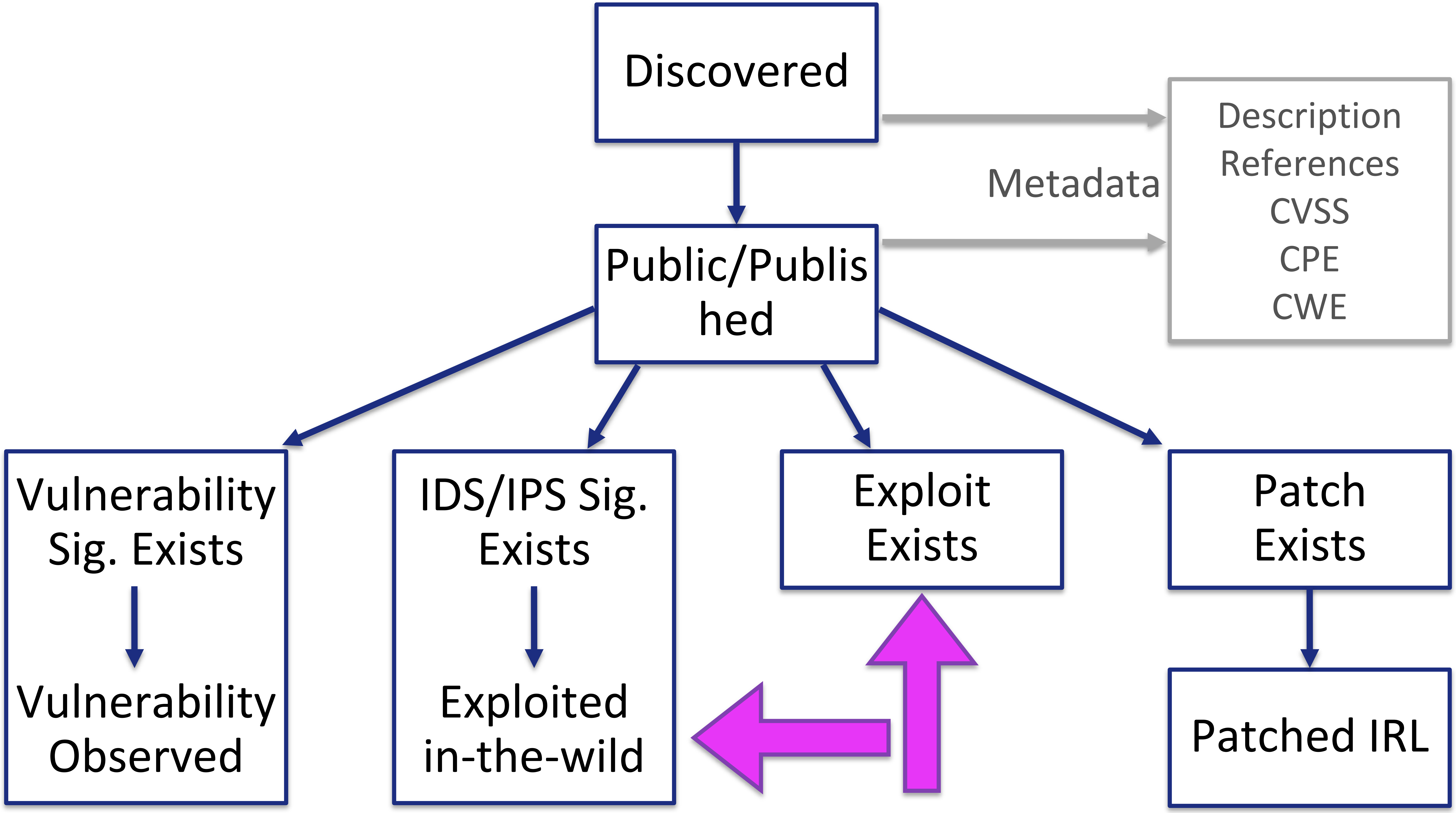
Source: Kenna / Cyentia

Things Happen Quick

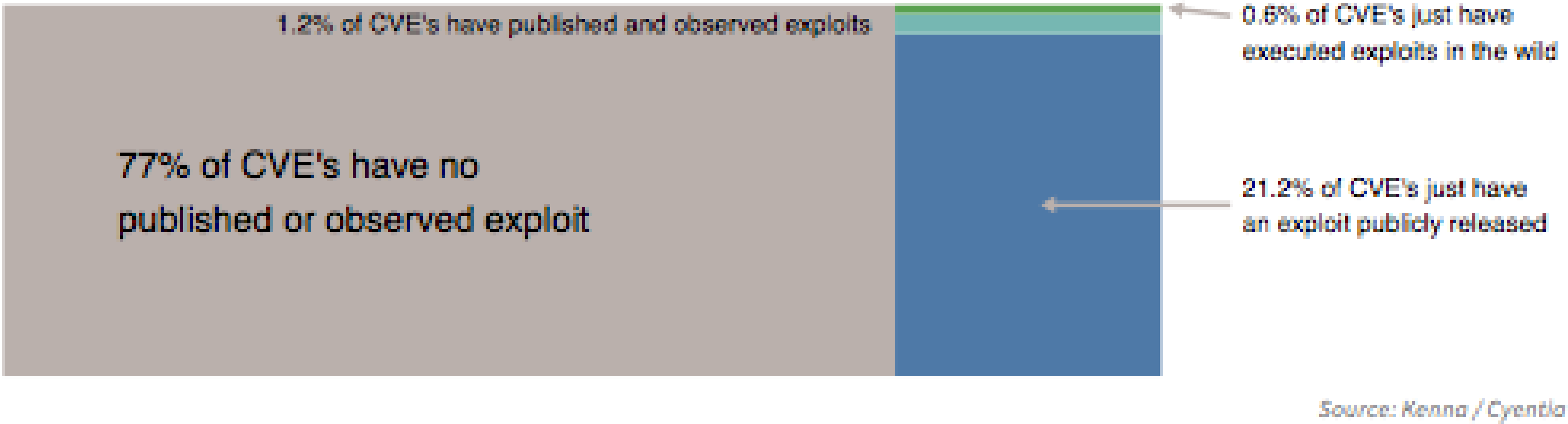
CVEs with Published Exploit
20%
15%
10%
5%
0%
-1 year
-6 months
CVE Published
6 months
1 year

Source: Kenna / Cyentia

Simplified View of Vulnerabilities



The World of CVEs (counting by CVEs)



1.2% of CVE's have published and observed exploits

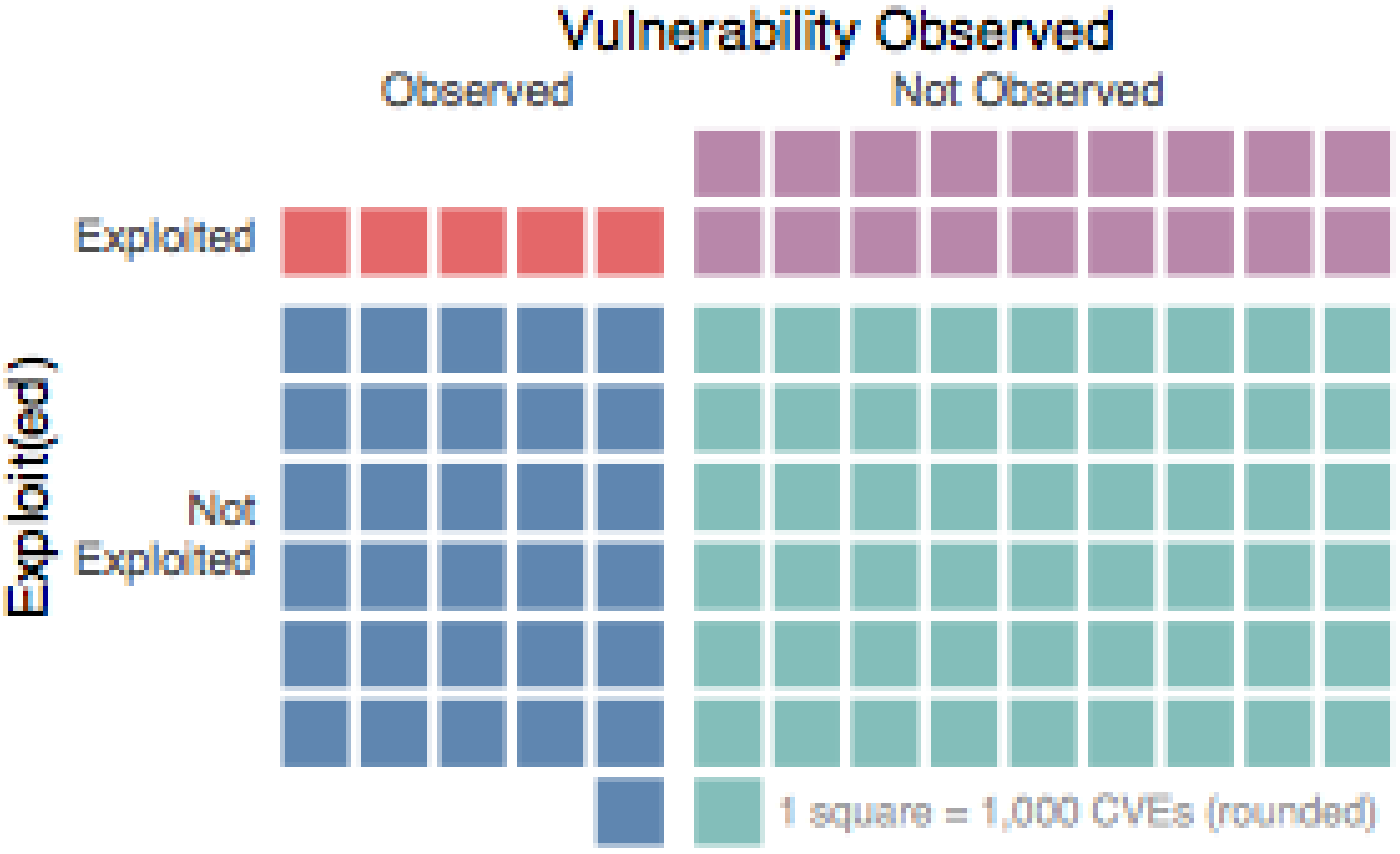
0.6% of CVE's just have executed exploits in the wild

77% of CVE's have no published or observed exploit

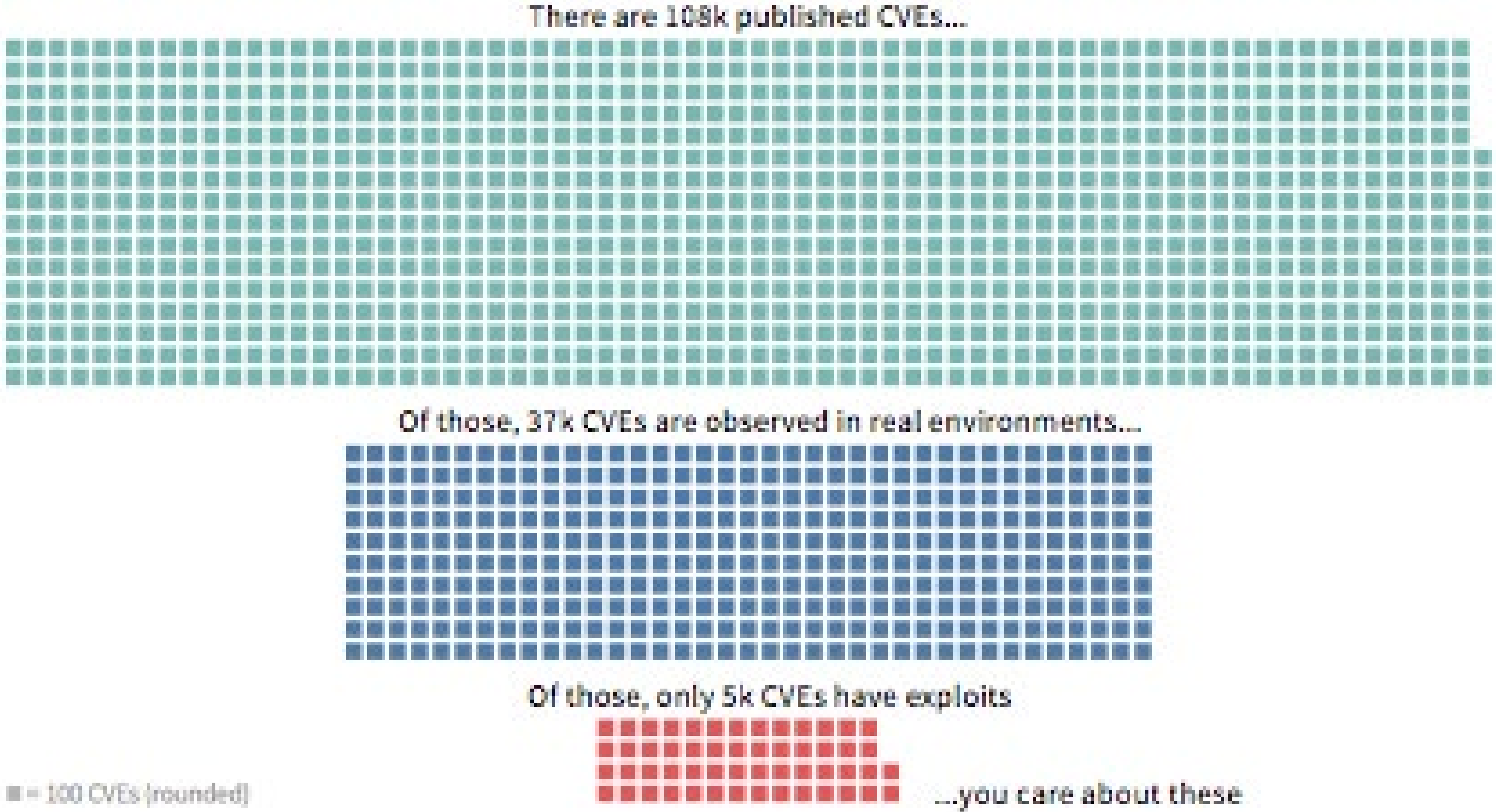
21.2% of CVE's just have an exploit publicly released

Source: Kenna / Cyentia

Published CVEs



Published CVEs



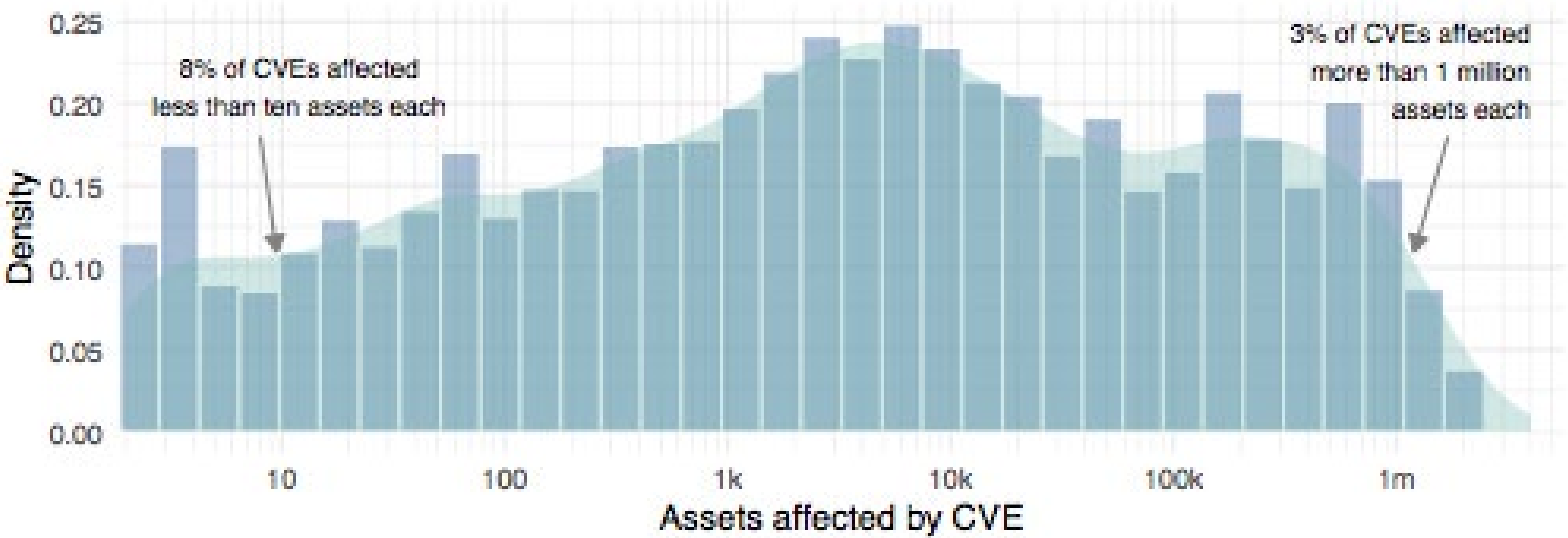
There are 108k published CVEs...

Of those, 37k CVEs are observed in real environments...

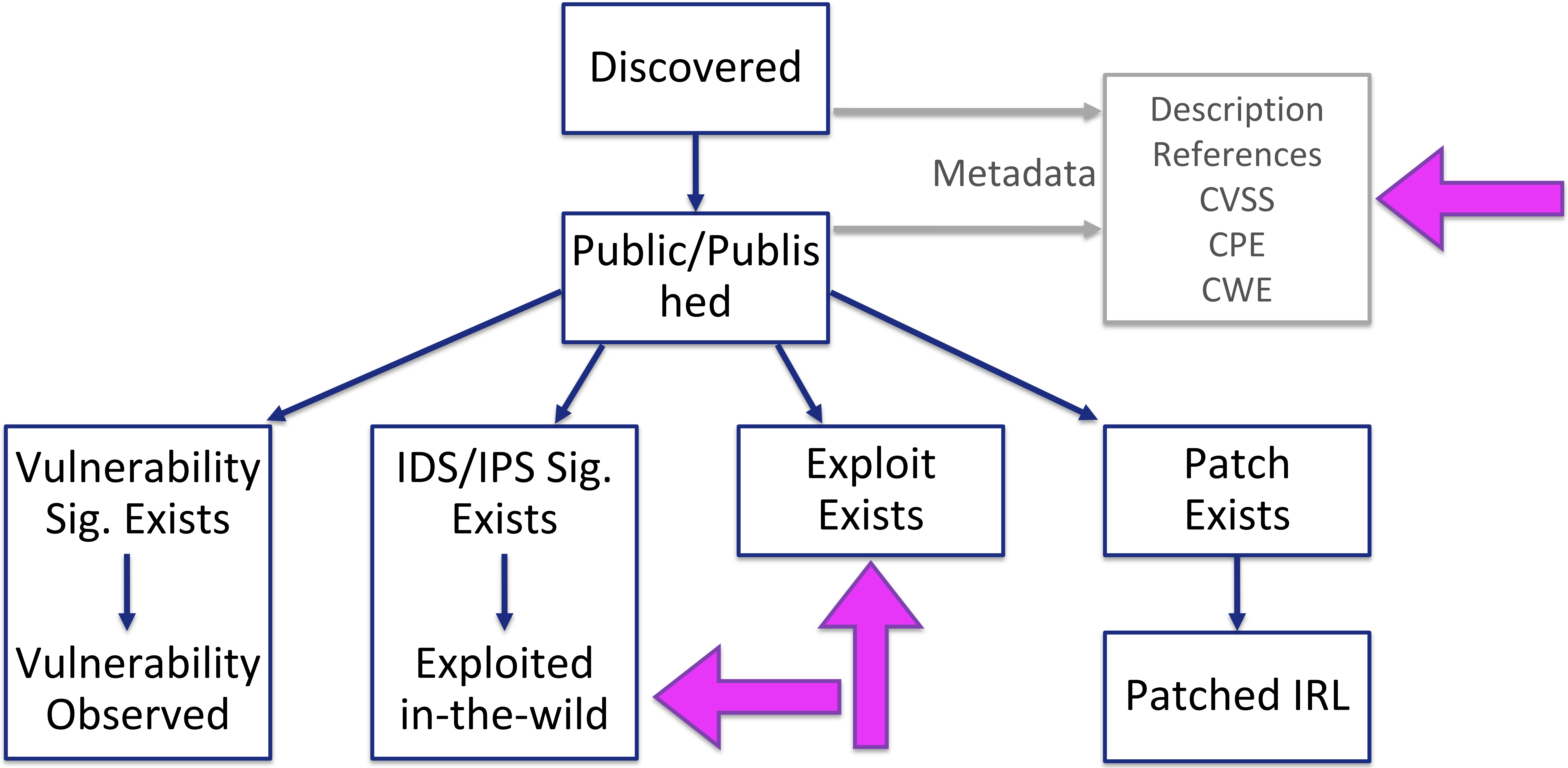
Of those, only 5k CVEs have exploits

...you care about these

What about Volume of Open Vulns?



Simplified View of Vulnerabilities



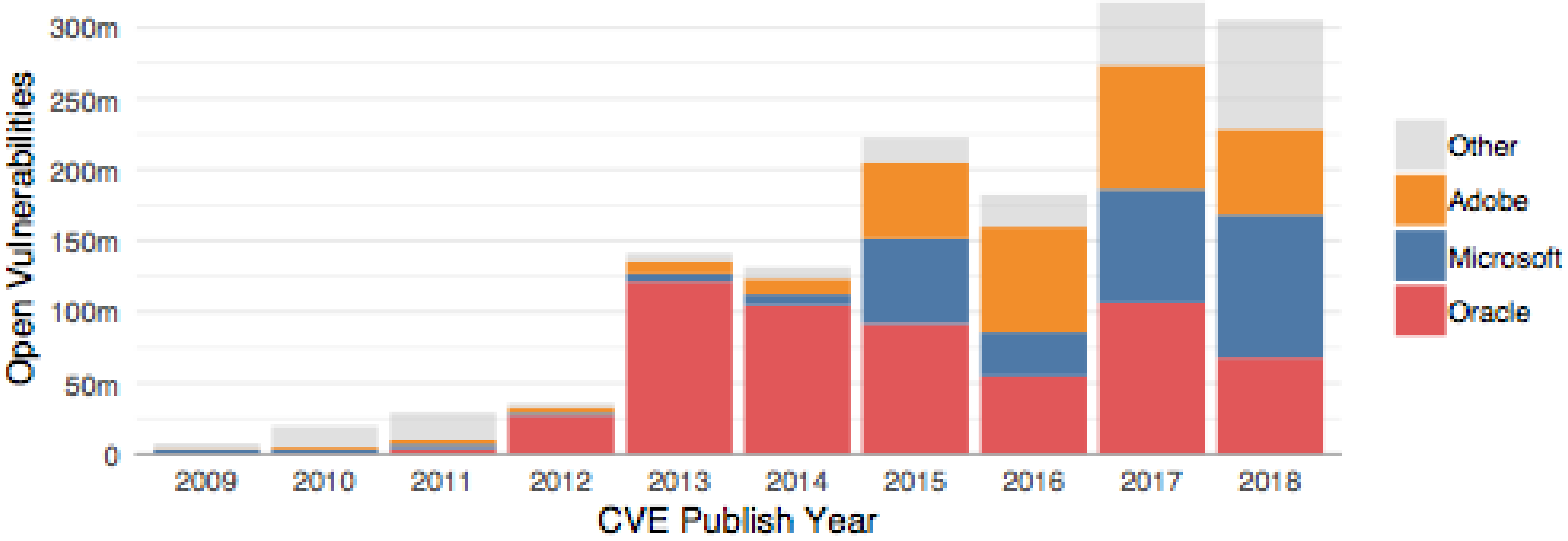
Is CVSS used to prioritize IRL?

Vulnerabilities
600m
500m
400m
300m
200m
100m
0
<0.01%
<0.01%
3.1%
2.3%
16.0%
19.2%
3.7%
12.0%
8.9%
16.9%
17.6%
0
1
2
3
4
5
6
7
8
9
10
CVSS Score

The Vendor Role in Remediation?

Percent of Open Vulnerabilities
0.0%
10.0%
20.0%
30.0%
34.4%
17.6%
17.1%
5.1%
3.3%
3.1%
2.0%
1.9%
1.9%
1.6%
Oracle
Microsoft
Adobe
IBM
Debian
Canonical
Mozilla
Apple
Google
Opensuse

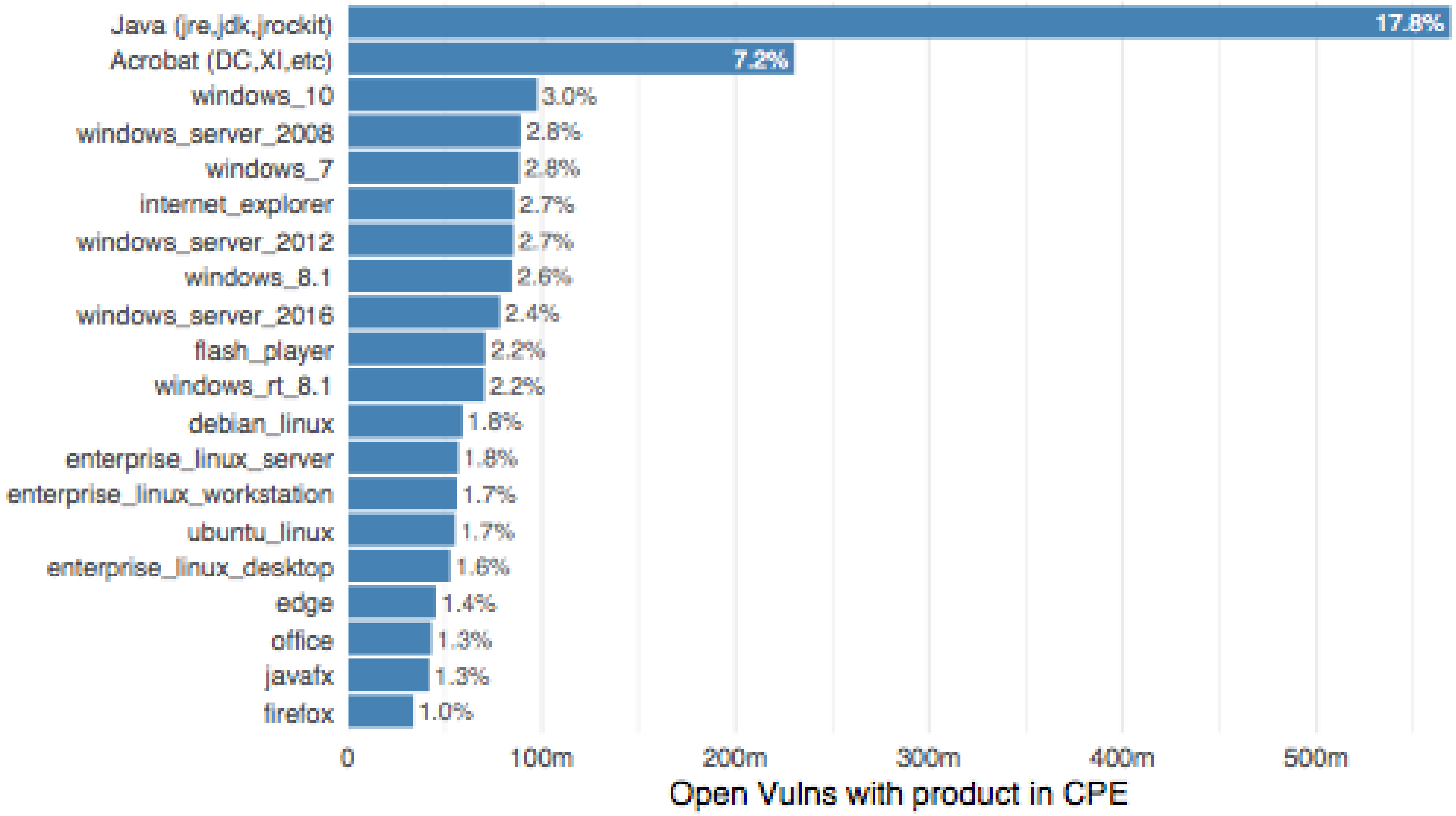
Top 3 Vendors



Top 3 Vendors

Open
Closed
Oracle
578m
259m
Adobe
303m
544m
Microsoft
296m
1b
0
500m
1b
Count of vulnerabilities
vendor
Open
Closed
Oracle
69.1%
30.9%
Adobe
35.8%
64.2%
Microsoft
22.4%
77.6%
0%
25%
50%
75%
100%
Percent of CVEs

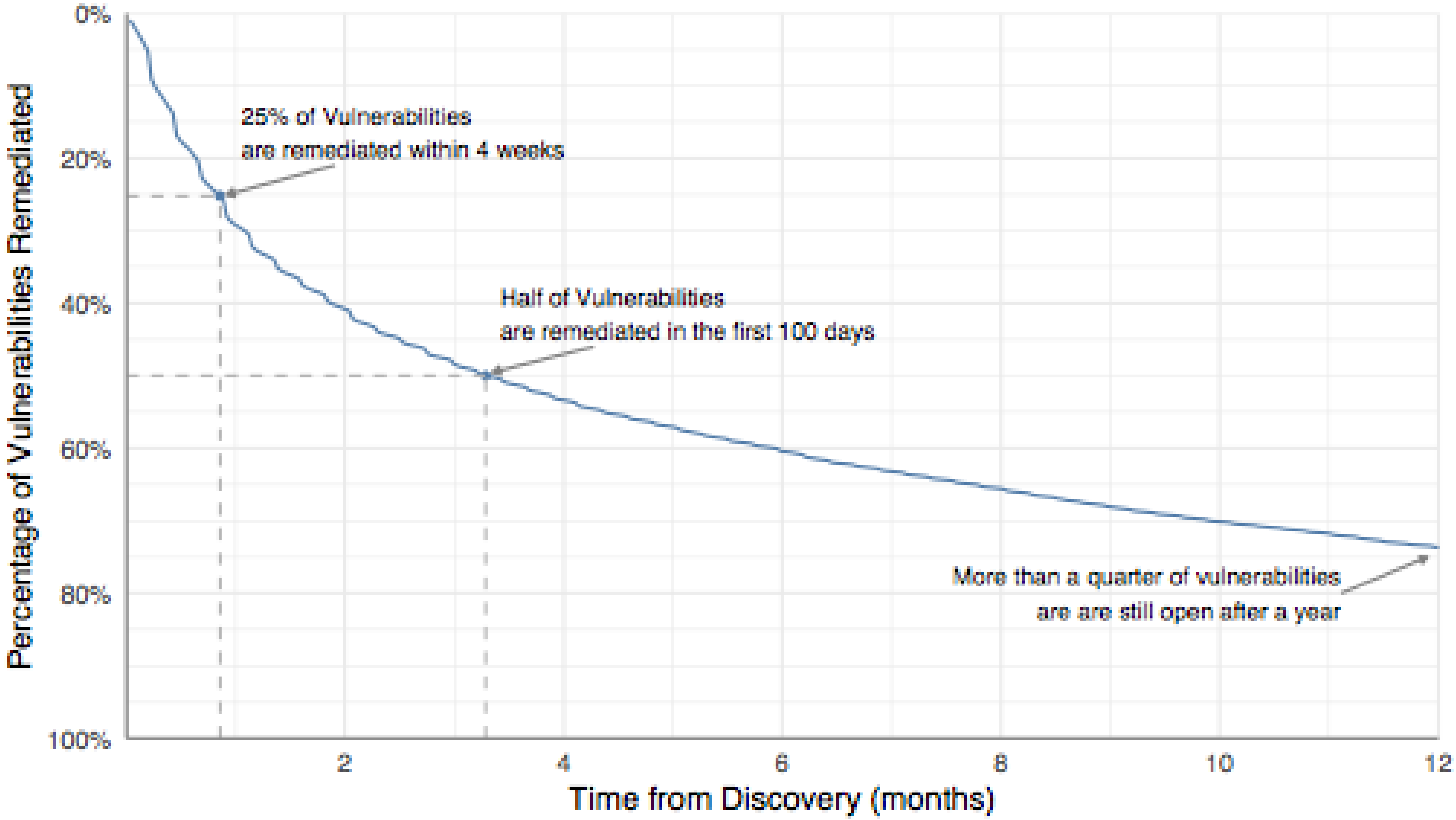
Top Products going unpatched



RSA Conference2019

A Quick aside on remediation times…

Probability of Patching

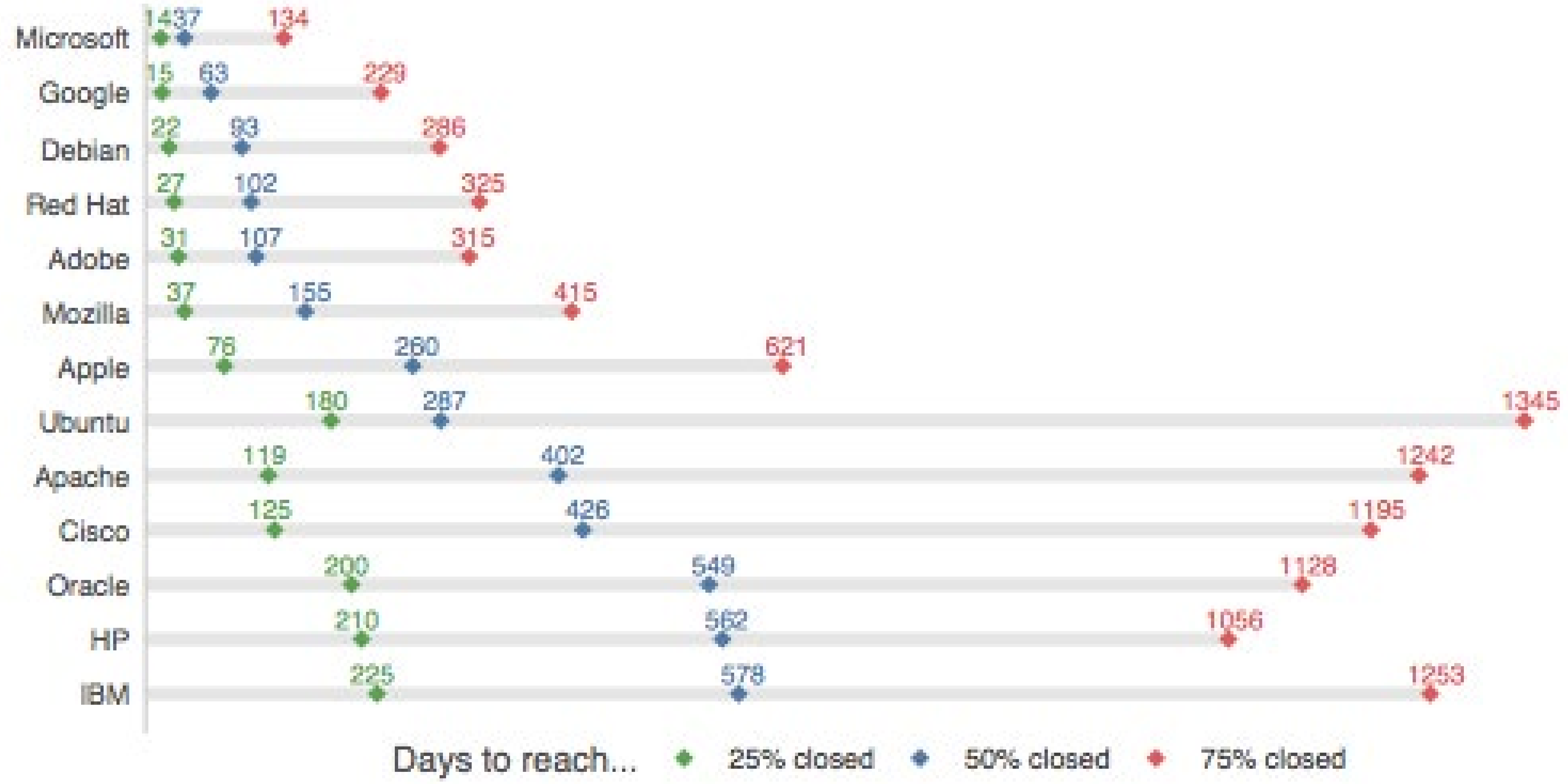


25% of Vulnerabilities
are remediated within 4 weeks

Half of Vulnerabilities
are remediated in the first 100 days

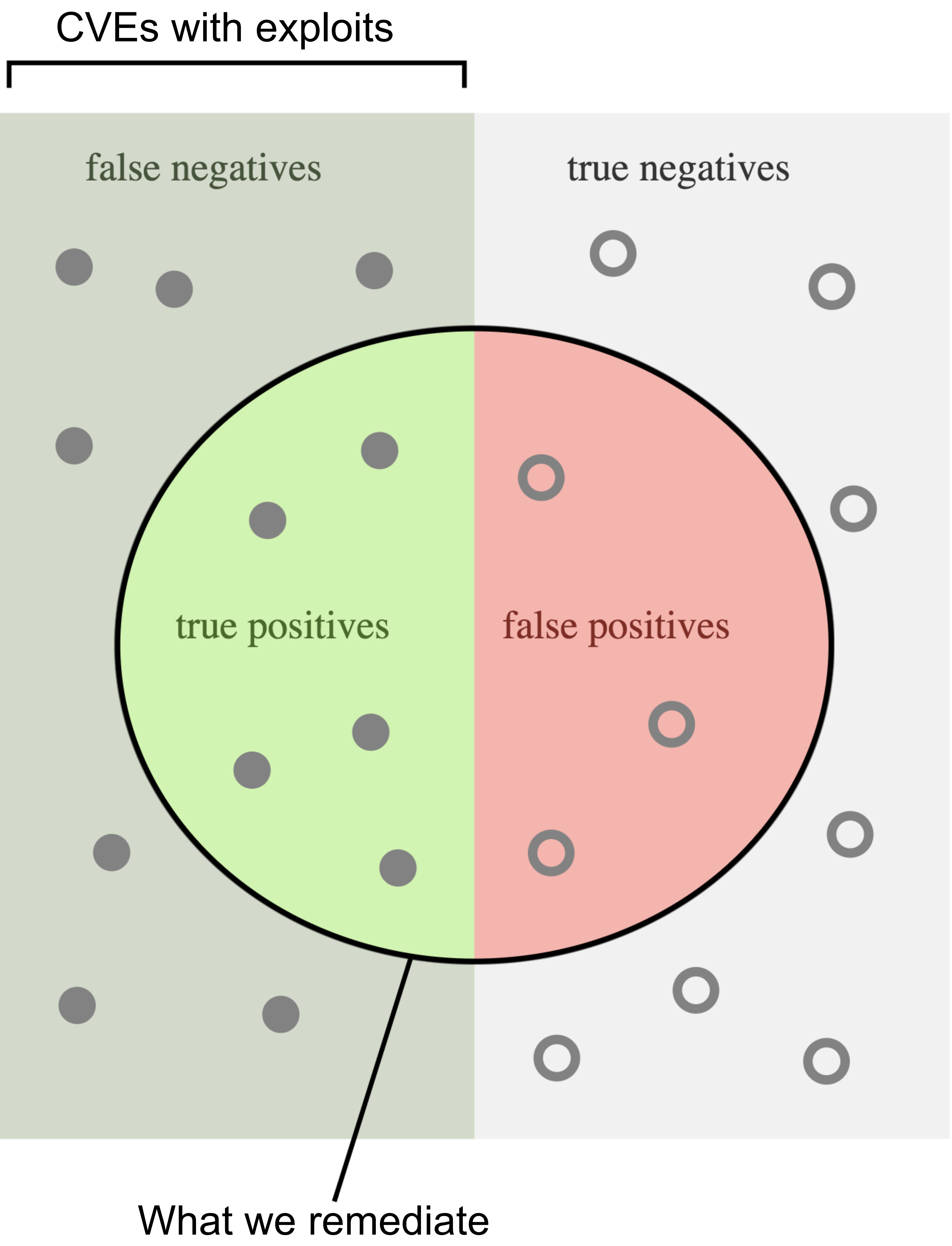
More than a quarter of vulnerabilities
are are still open after a year

The Case for Auto-Patching



How effective is your remediation strategy?

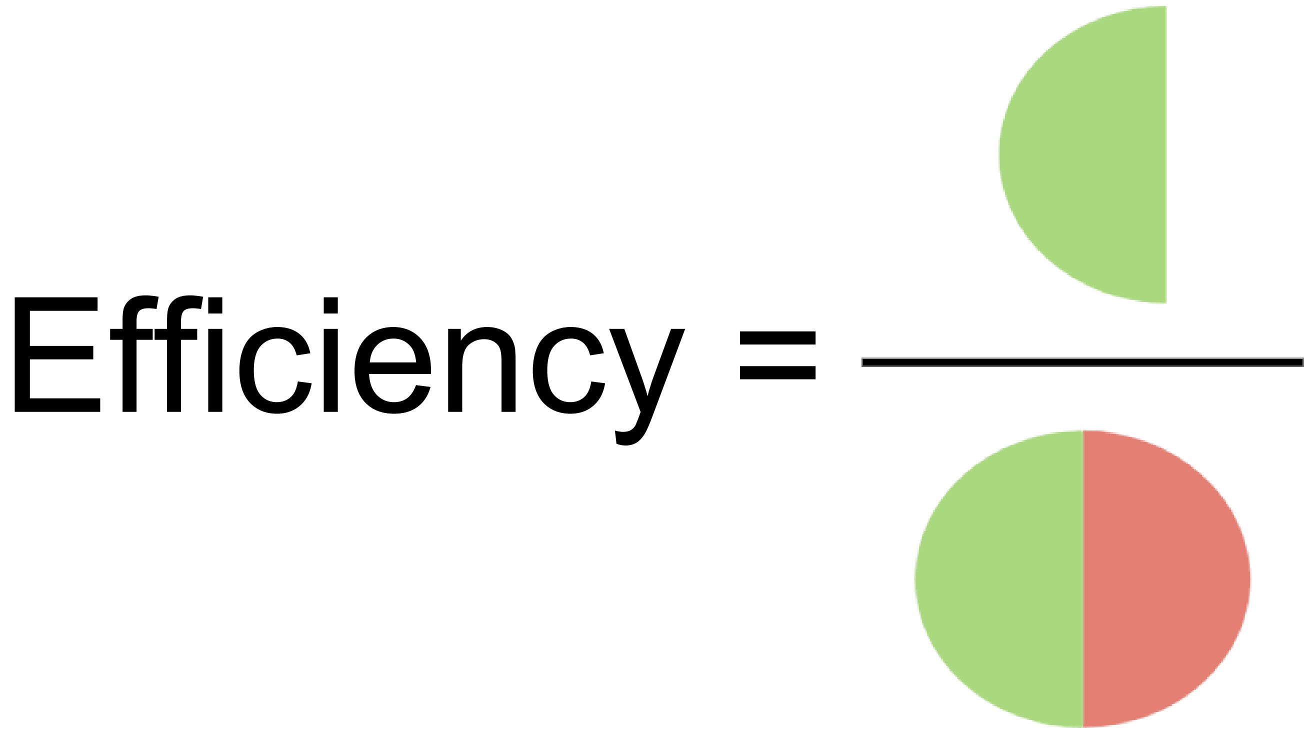
Measuring Remediation Decisions



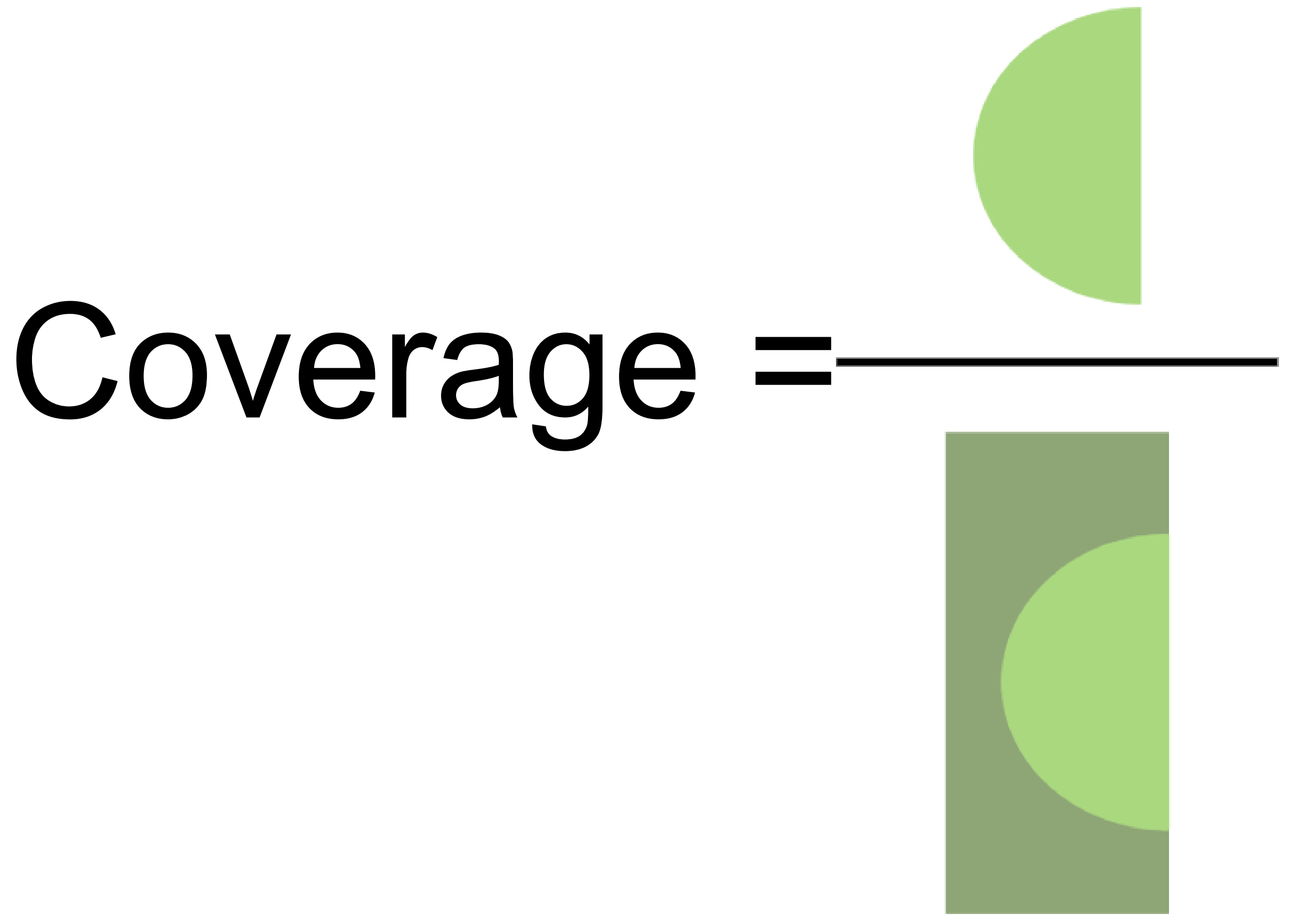
Efficiency and Coverage

(Precision and Recall)

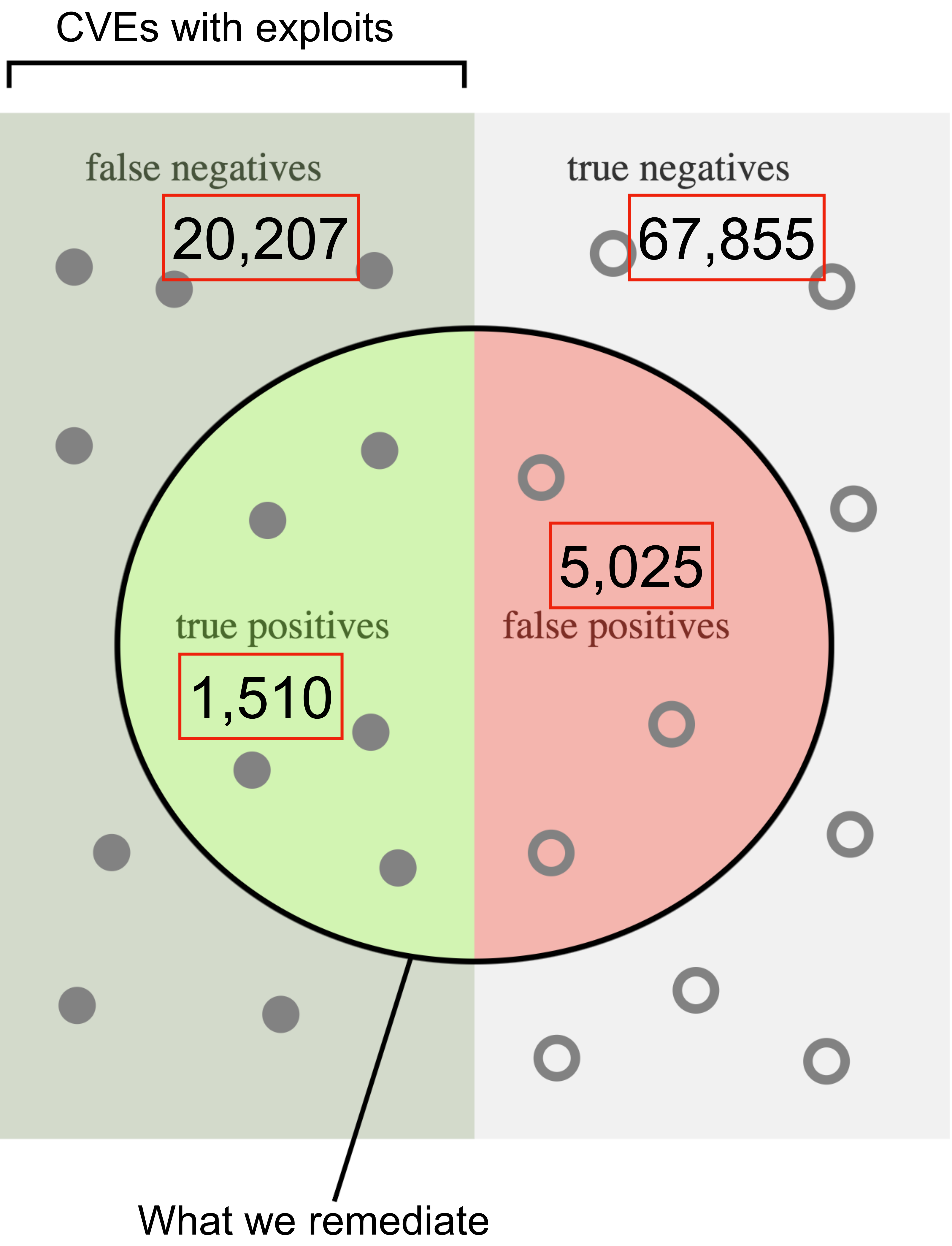
How many remediated CVEs have published exploits?



How many CVEs with published exploits have been remediated?

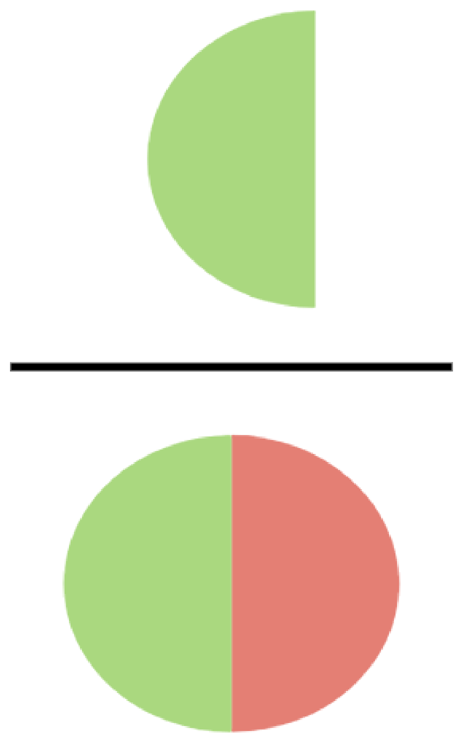


Measuring Decisions: CVSS 10



How many remediated CVEs have published exploits?

Efficiency =

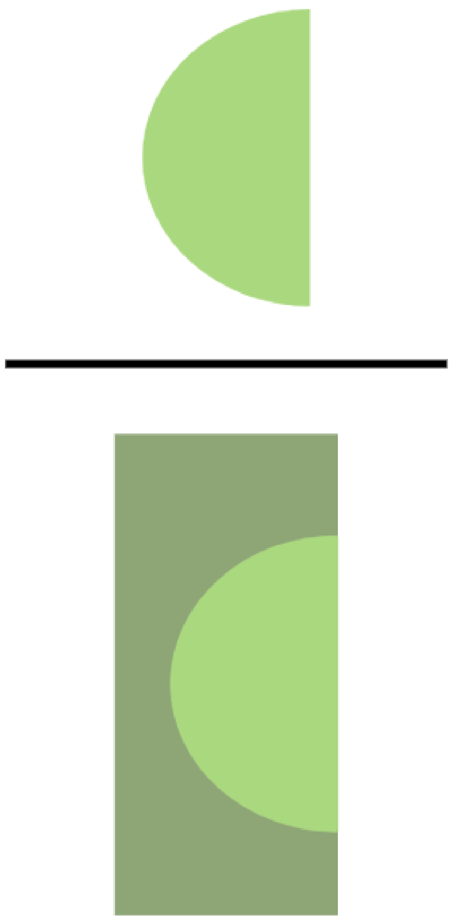


$$= \frac{1{,}510}{1{,}510 + 5{,}025}$$

23.1% Efficiency

How many CVEs with published exploits have been remediated?

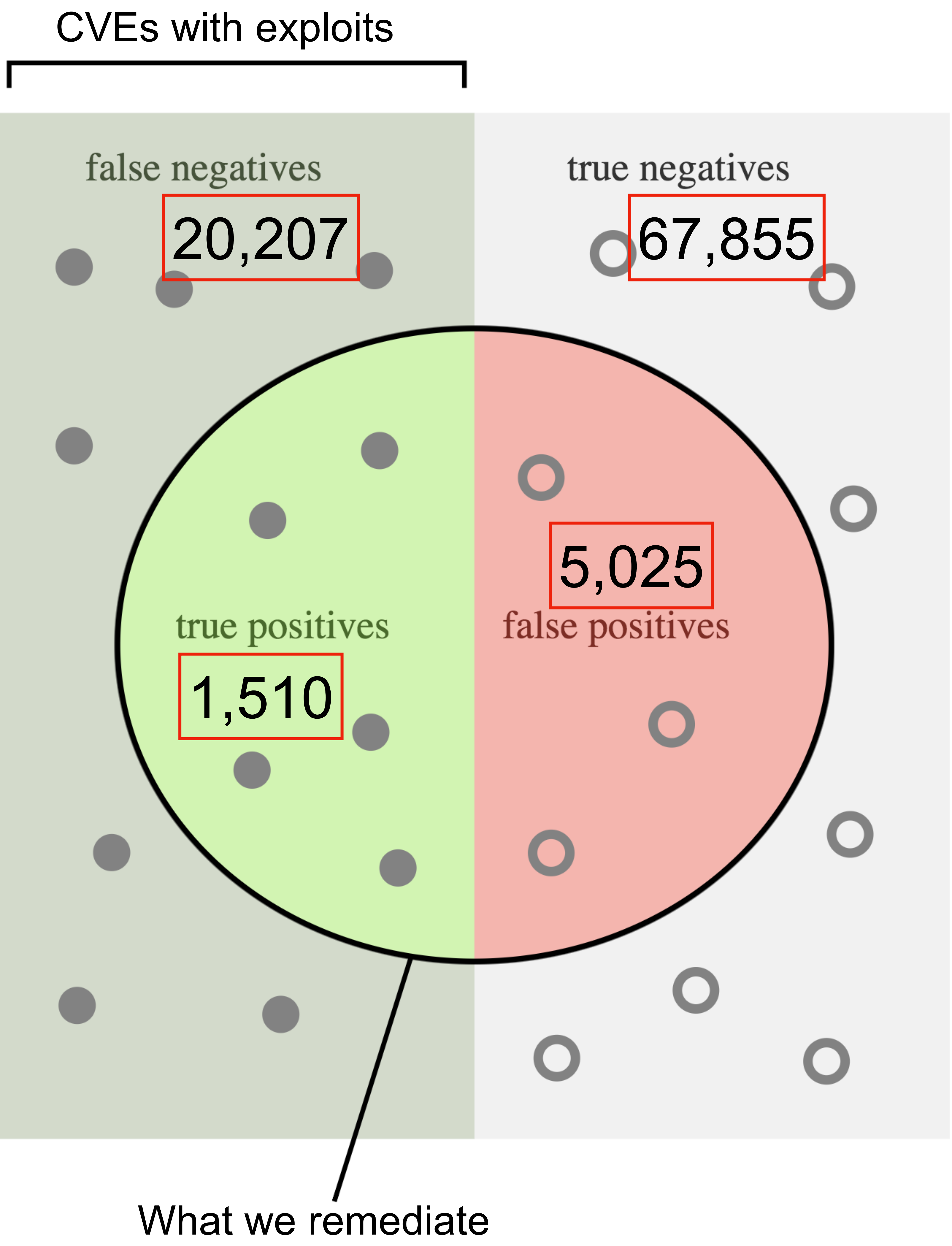
Coverage =



$$= \frac{1{,}510}{1{,}510 + 20{,}207}$$

7% Coverage

Measuring Decisions: CVSS 10



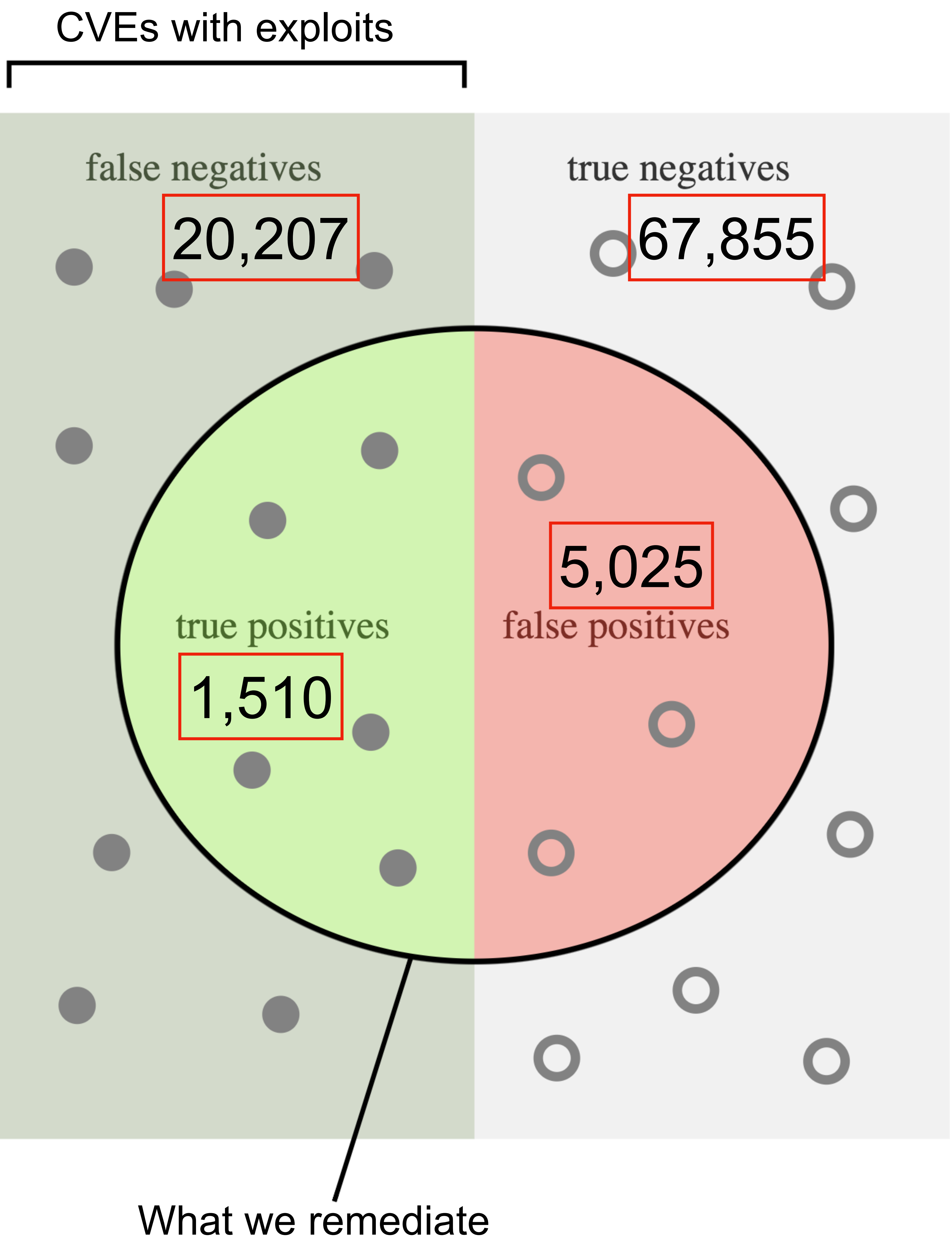
Remediating CVSS 10+ results in:

6,535 CVEs prioritized,

23.1% Efficiency, 7% Coverage

Is this good?

Measuring Decisions: CVSS 10



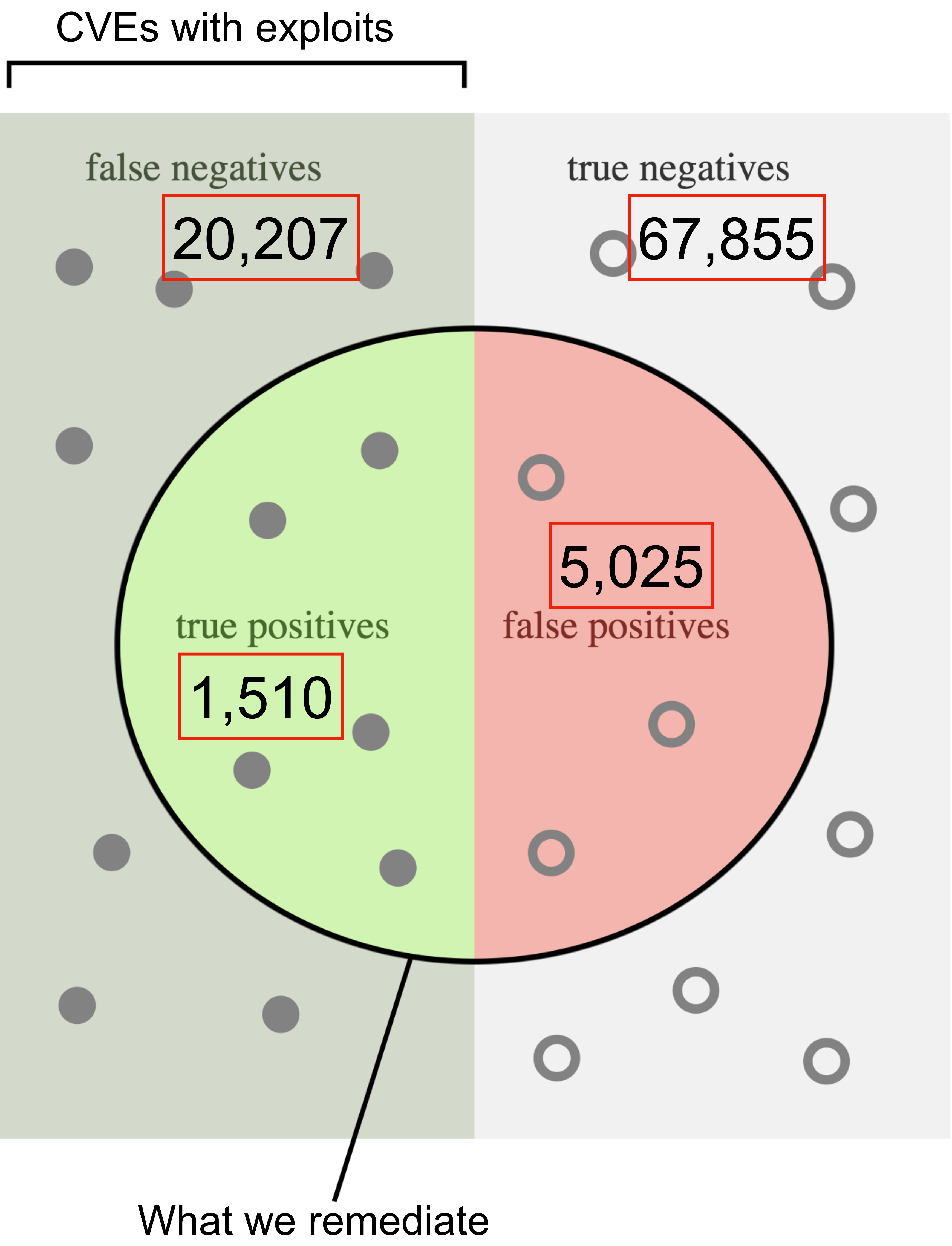
Remediating CVSS 10+ results in:

6,535 CVEs prioritized,
23.1% Efficiency, 7% Coverage

Is this good?

What if we randomly selected 6,535 CVEs to remediate?

Measuring Decisions: CVSS 10



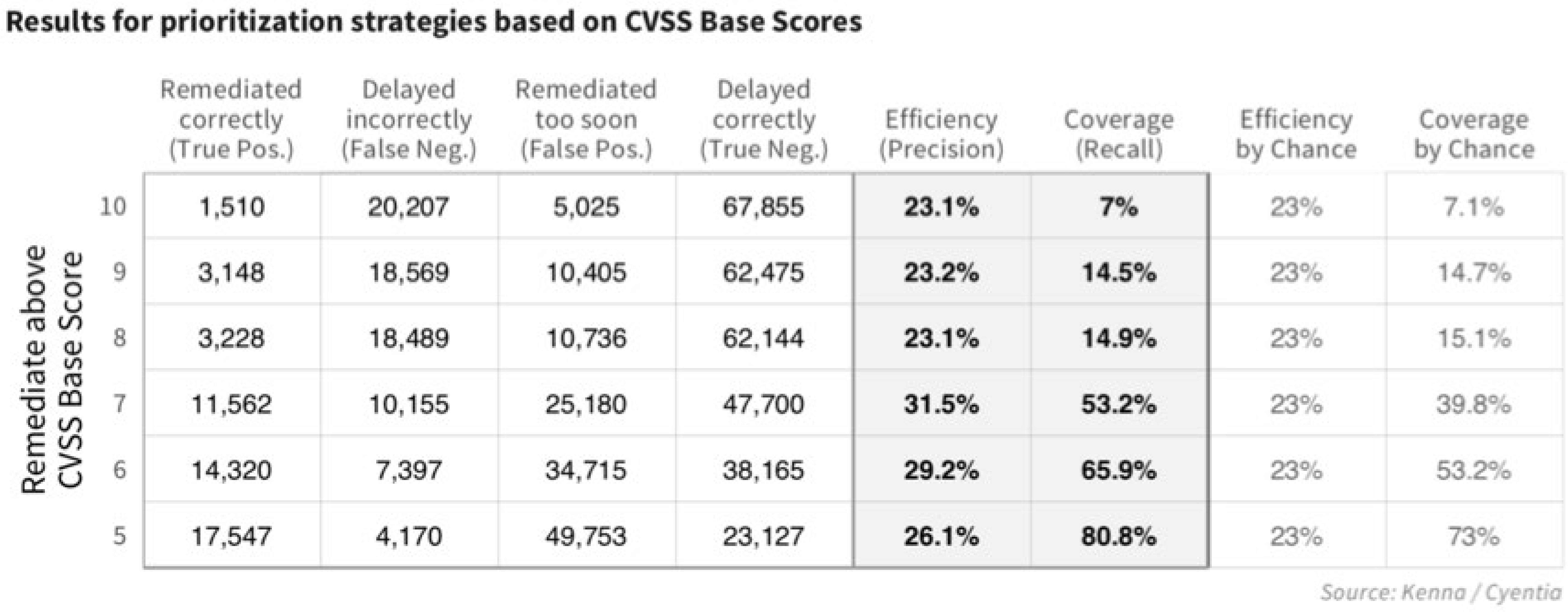
Remediating CVSS 10+ results in:
6,535 CVEs prioritized,
23.1% Efficiency, 7% Coverage

Is this good?

What if we randomly selected 6,535 CVEs to remediate?

23% Efficiency, 7.1% Coverage

Measuring Decisions: CVSS

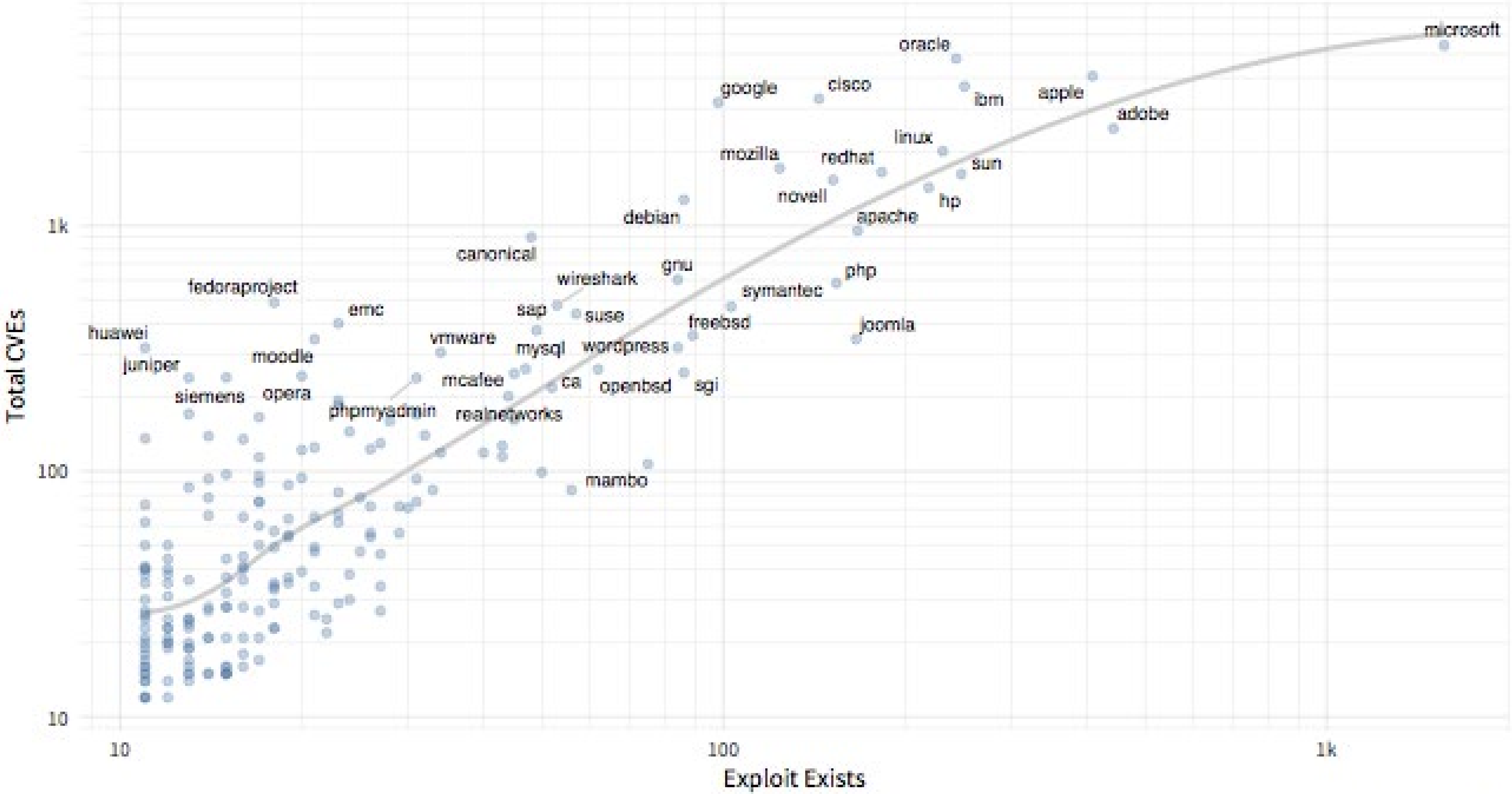


Results for prioritization strategies based on CVSS Base Scores

Remediate above CVSS Base Score	Remediated correctly (True Pos.)	Delayed incorrectly (False Neg.)	Remediated too soon (False Pos.)	Delayed correctly (True Neg.)	Efficiency (Precision)	Coverage (Recall)	Efficiency by Chance	Coverage by Chance
10	1,510	20,207	5,025	67,855	**23.1%**	**7%**	23%	7.1%
9	3,148	18,569	10,405	62,475	**23.2%**	**14.5%**	23%	14.7%
8	3,228	18,489	10,736	62,144	**23.1%**	**14.9%**	23%	15.1%
7	11,562	10,155	25,180	47,700	**31.5%**	**53.2%**	23%	39.8%
6	14,320	7,397	34,715	38,165	**29.2%**	**65.9%**	23%	53.2%
5	17,547	4,170	49,753	23,127	**26.1%**	**80.8%**	23%	73%

Source: Kenna / Cyentia

Vendor-based Strategy



Source: Kenna / Cyentia

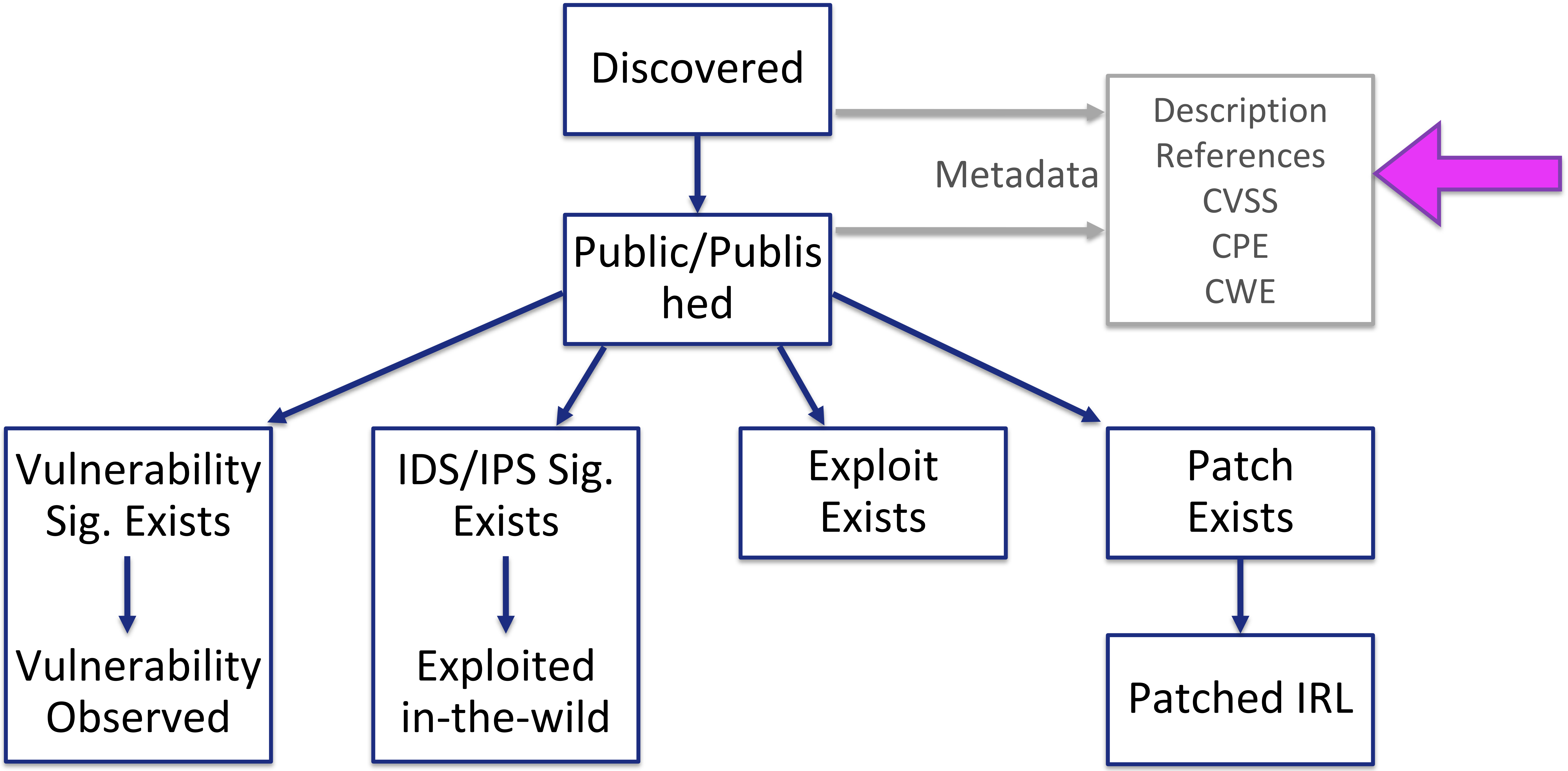
Vendor-based Strategy

Results for prioritization strategies based on vendors with the highest numbers of CVEs

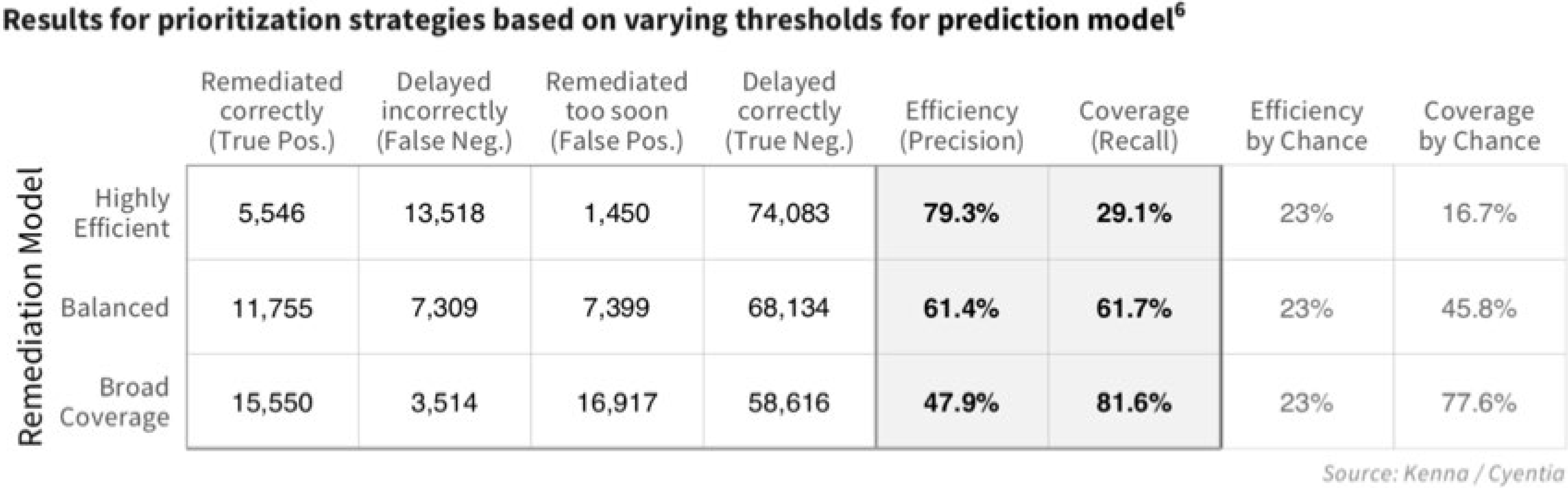
		Remediated correctly (True Pos.)	Delayed incorrectly (False Neg.)	Remediated too soon (False Pos.)	Delayed correctly (True Neg.)	Efficiency (Precision)	Coverage (Recall)	Efficiency by Chance	Coverage by Chance
Remediate Vendors	Top5	2,598	19,119	18,500	54,380	**12.3%**	**12%**	23%	22.9%
	Top10	3,588	18,129	27,705	45,175	**11.5%**	**16.5%**	23%	33.9%
	Top20	4,726	16,991	34,471	38,409	**12.1%**	**21.8%**	23%	42.5%

Source: Kenna / Cyentia

Simplified View of Vulnerabilities



Predictive Model

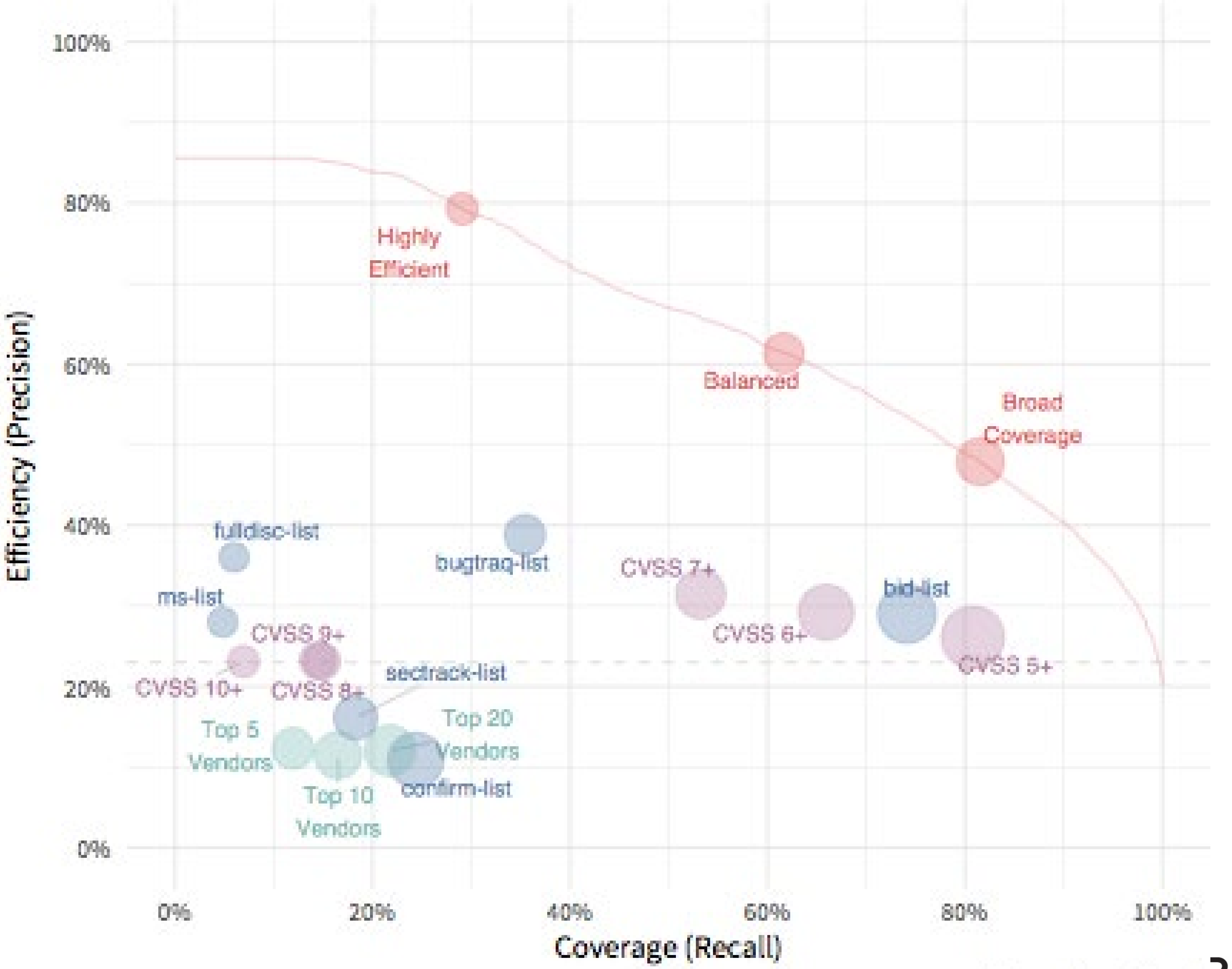


Results for prioritization strategies based on varying thresholds for prediction model[6]

		Remediated correctly (True Pos.)	Delayed incorrectly (False Neg.)	Remediated too soon (False Pos.)	Delayed correctly (True Neg.)	Efficiency (Precision)	Coverage (Recall)	Efficiency by Chance	Coverage by Chance
Remediation Model	Highly Efficient	5,546	13,518	1,450	74,083	**79.3%**	**29.1%**	23%	16.7%
	Balanced	11,755	7,309	7,399	68,134	**61.4%**	**61.7%**	23%	45.8%
	Broad Coverage	15,550	3,514	16,917	58,616	**47.9%**	**81.6%**	23%	77.6%

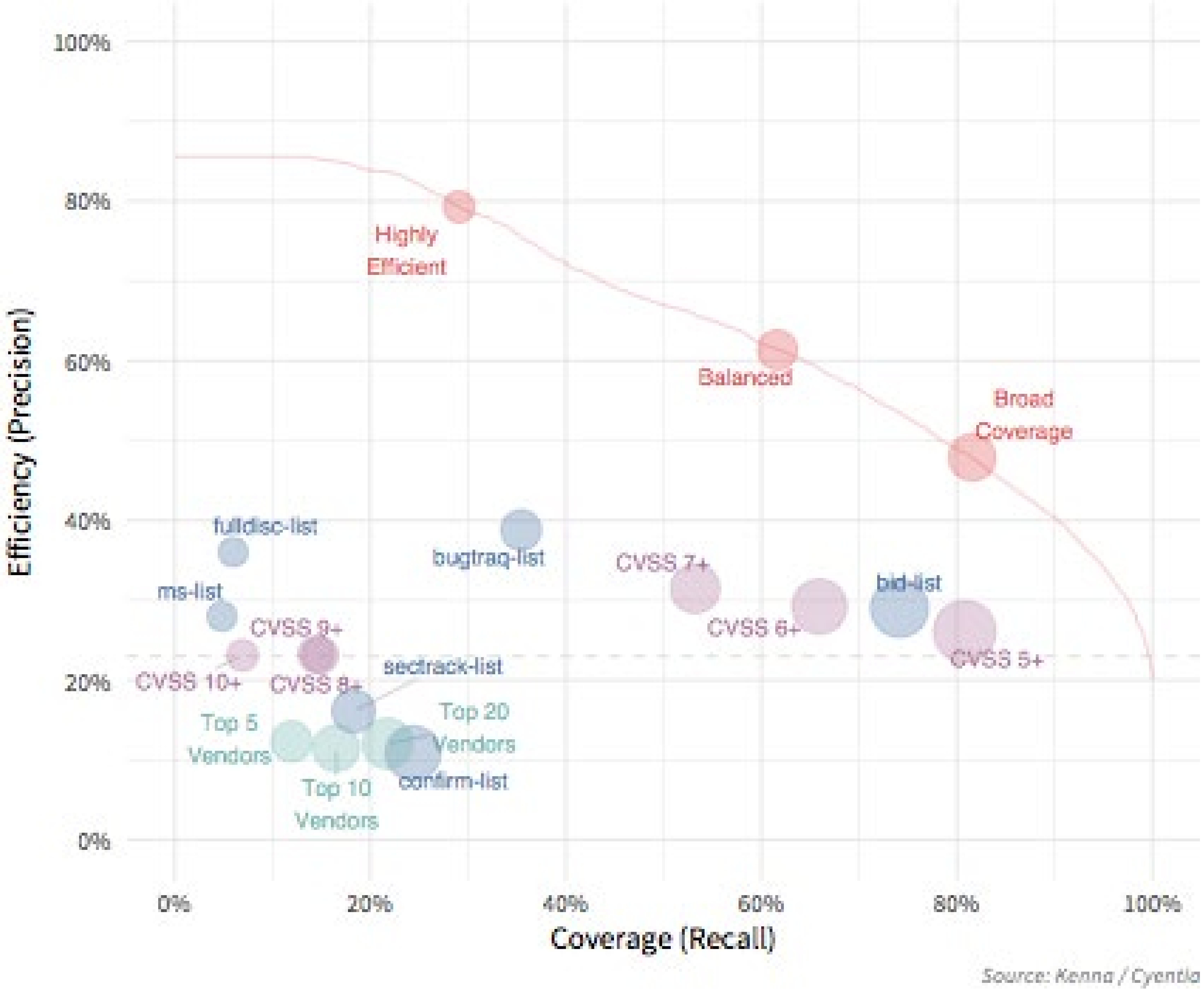
Source: Kenna / Cyentia

Predictive Model



Source: Kenna / Cyentia

Predictive Model



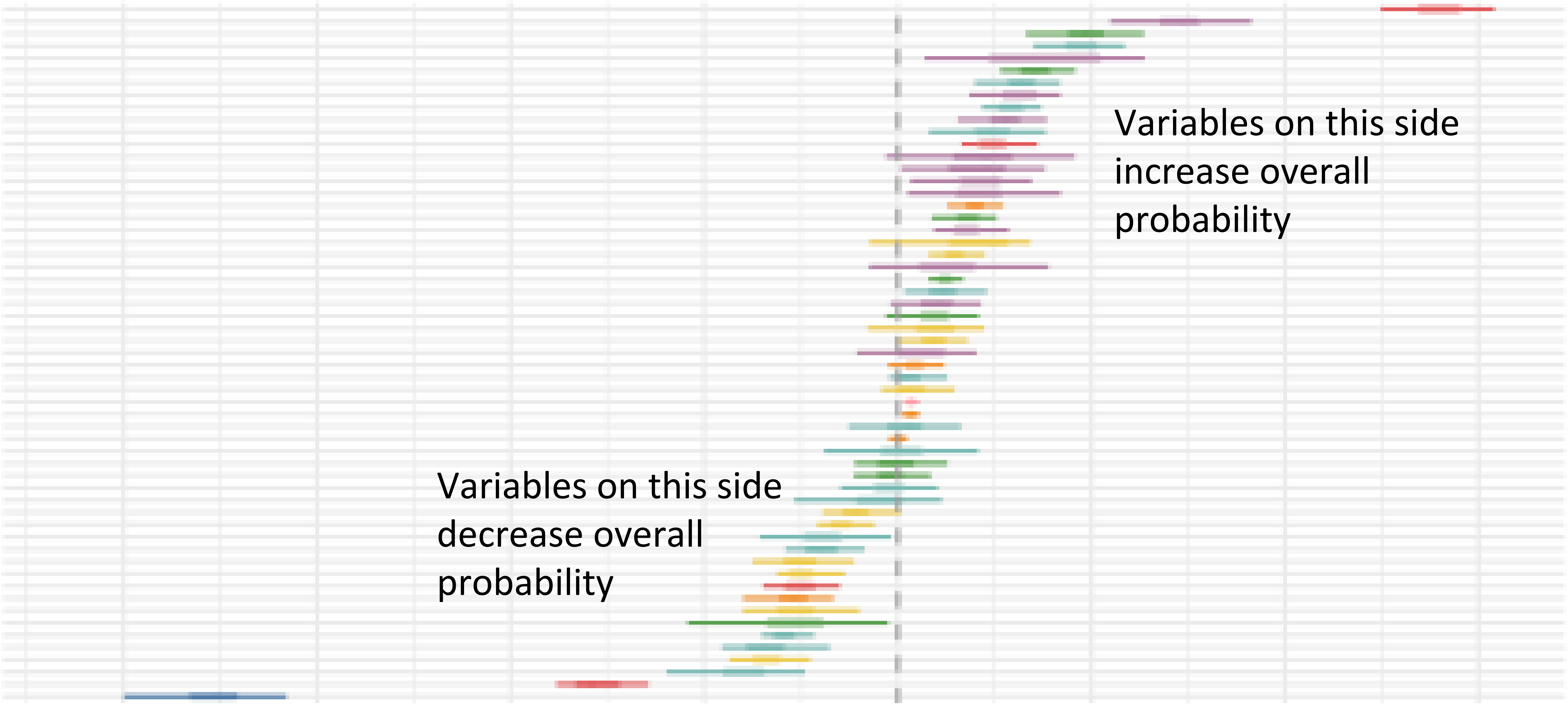
Source: Kenna / Cyentia

CVSS 7+ to "Balanced"

- Twice the efficiency
- Improved Coverage (53% to 62%)
- A Third of FP
- Half the effort

The Etiology of Vulnerability Exploitation

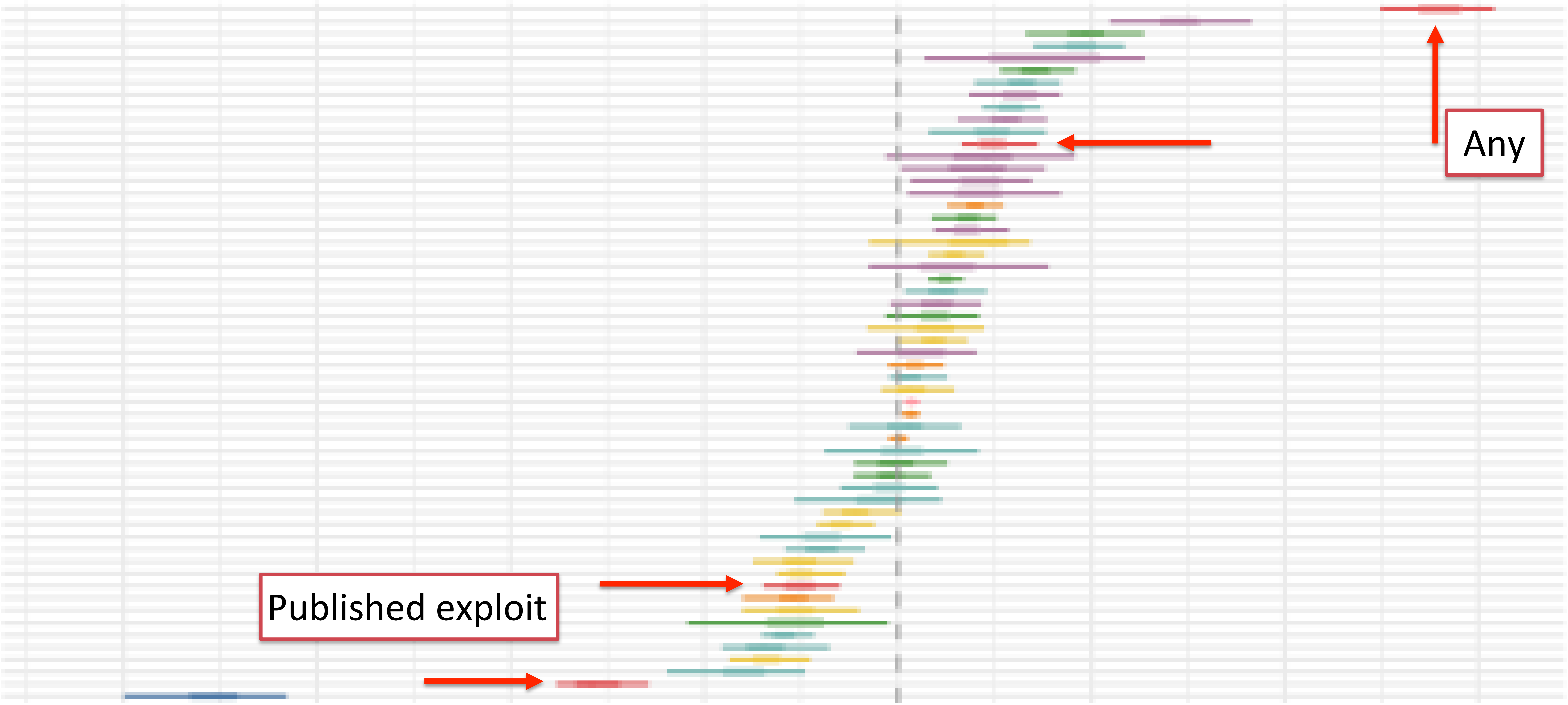
What contributes to exploitation in the wild?



Variables on this side increase overall probability

Variables on this side decrease overall probability

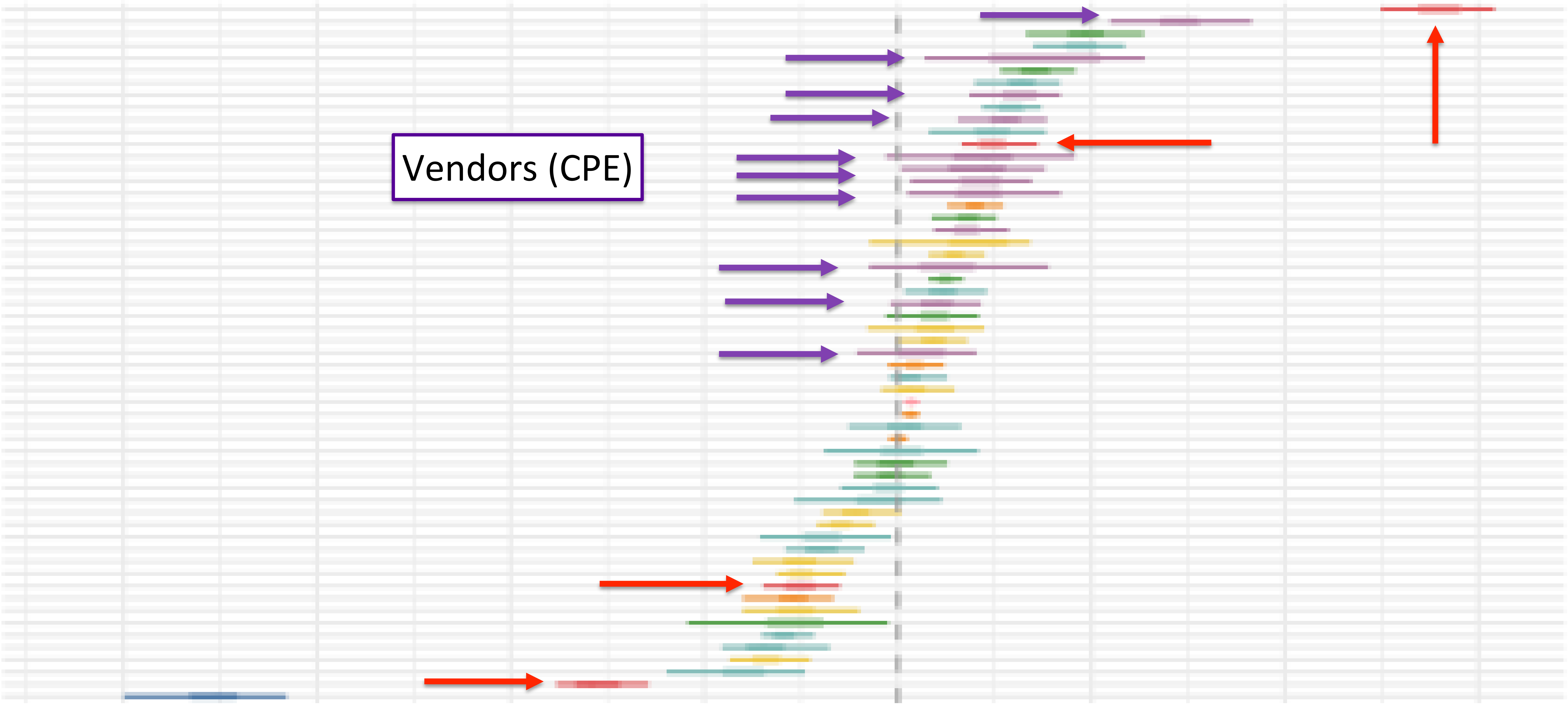
What contributes to exploitation in the wild?



Any

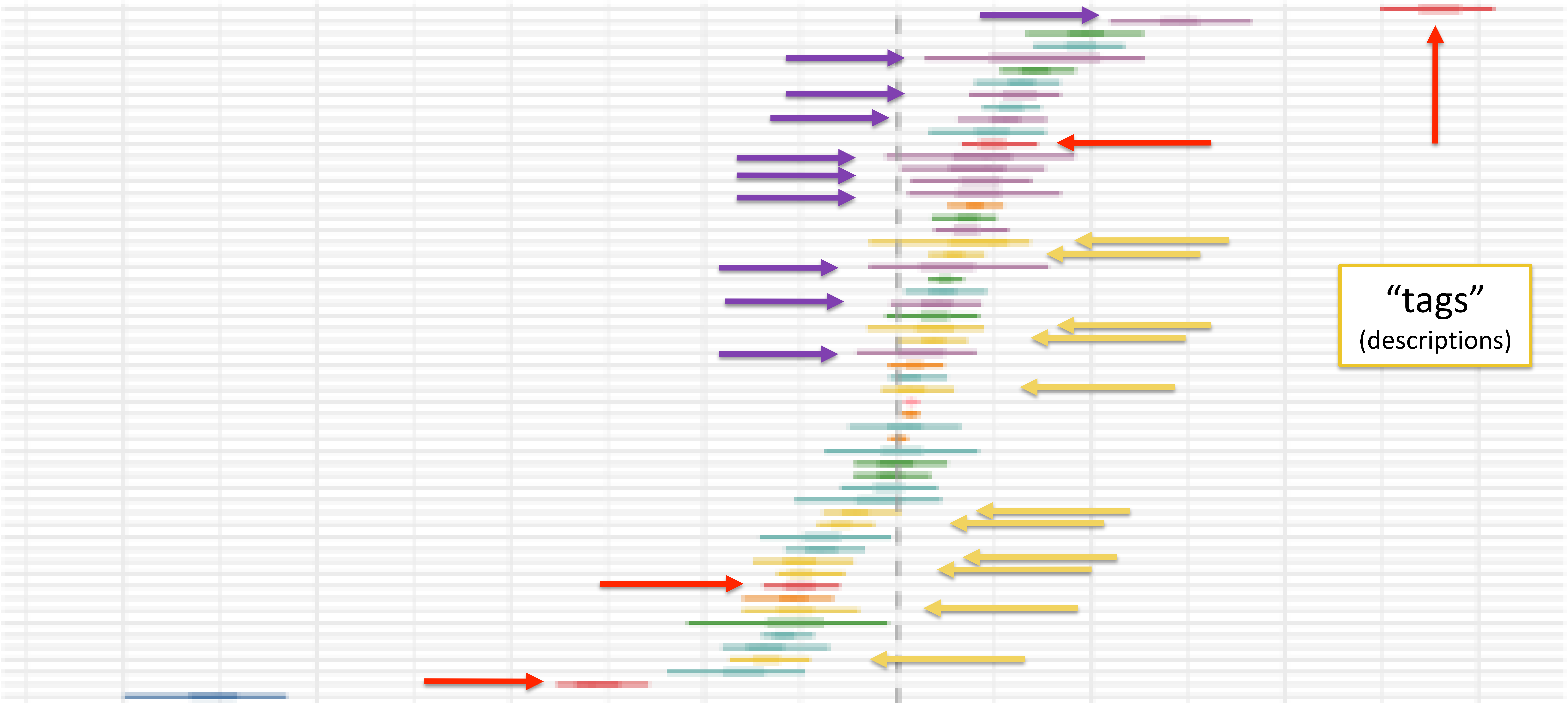
Published exploit

What contributes to exploitation in the wild?



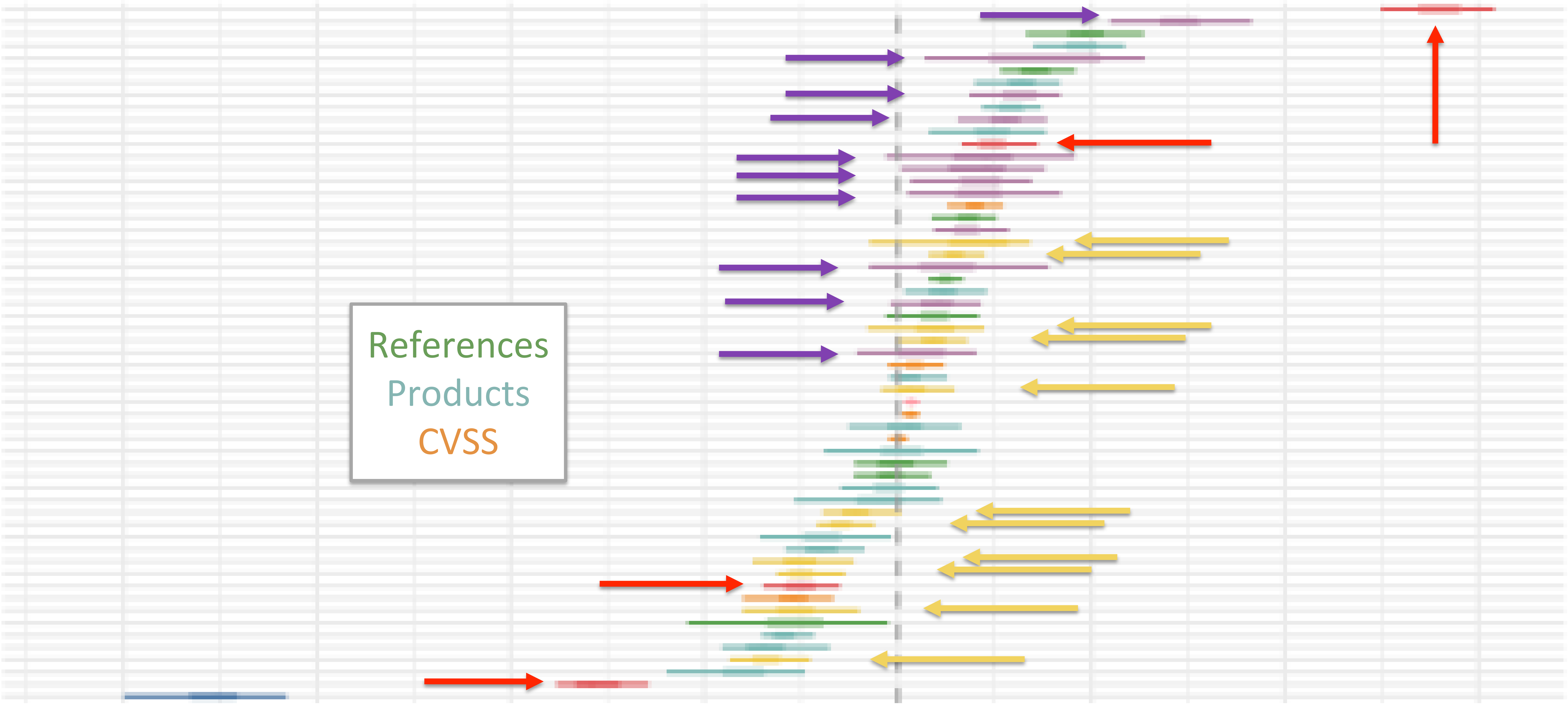
Vendors (CPE)

What contributes to exploitation in the wild?



“tags”
(descriptions)

What contributes to exploitation in the wild?



What contributes to exploitation in the wild?

If there is a published exploit, in metasploit: 40% chance

If nothing else is present, 0.1% chance of exploitation

What contributes to exploitation in the wild?

…AND has a CVE reference from MS: 81% chance

If there is a published exploit, in metasploit: 40% chance

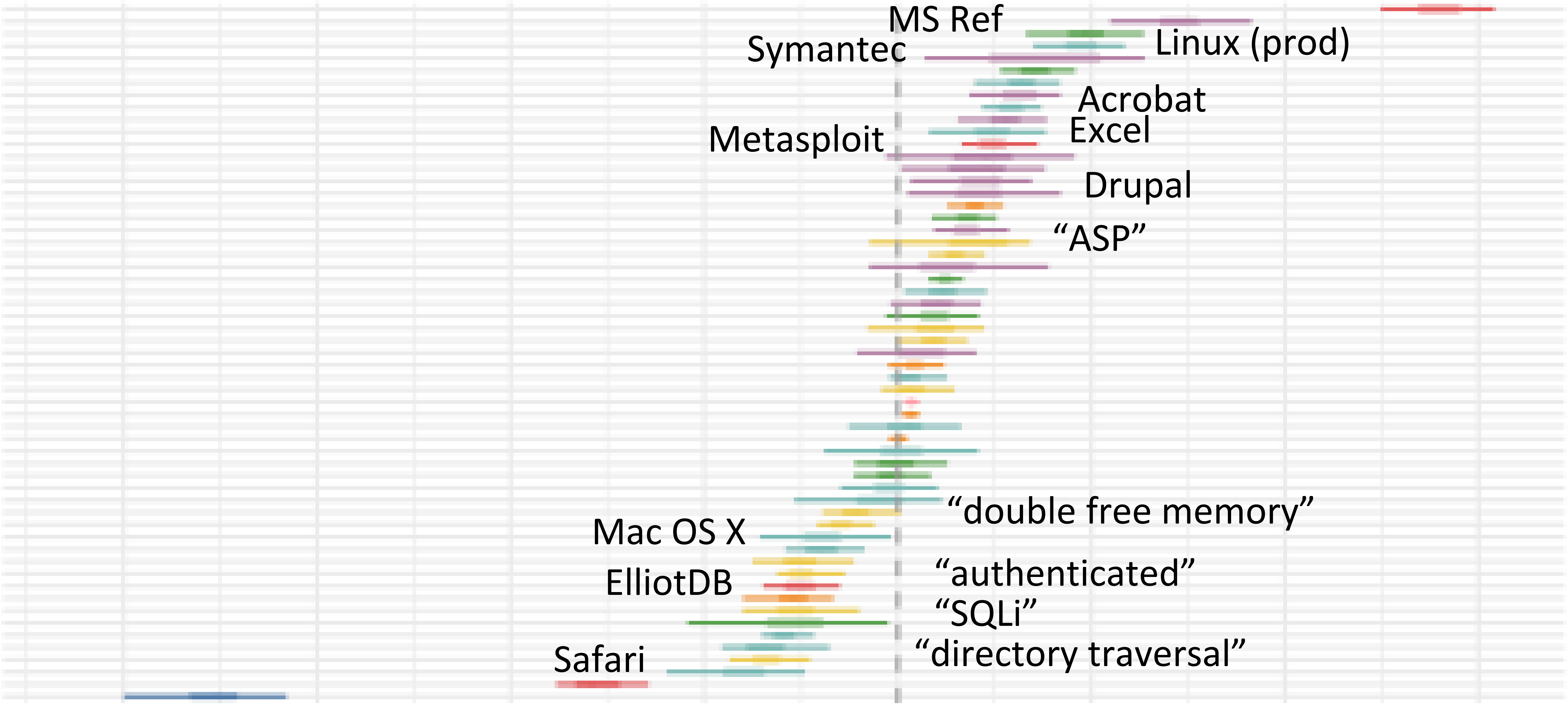
What contributes to exploitation in the wild?

...AND has a CVE reference from MS: 81% chance

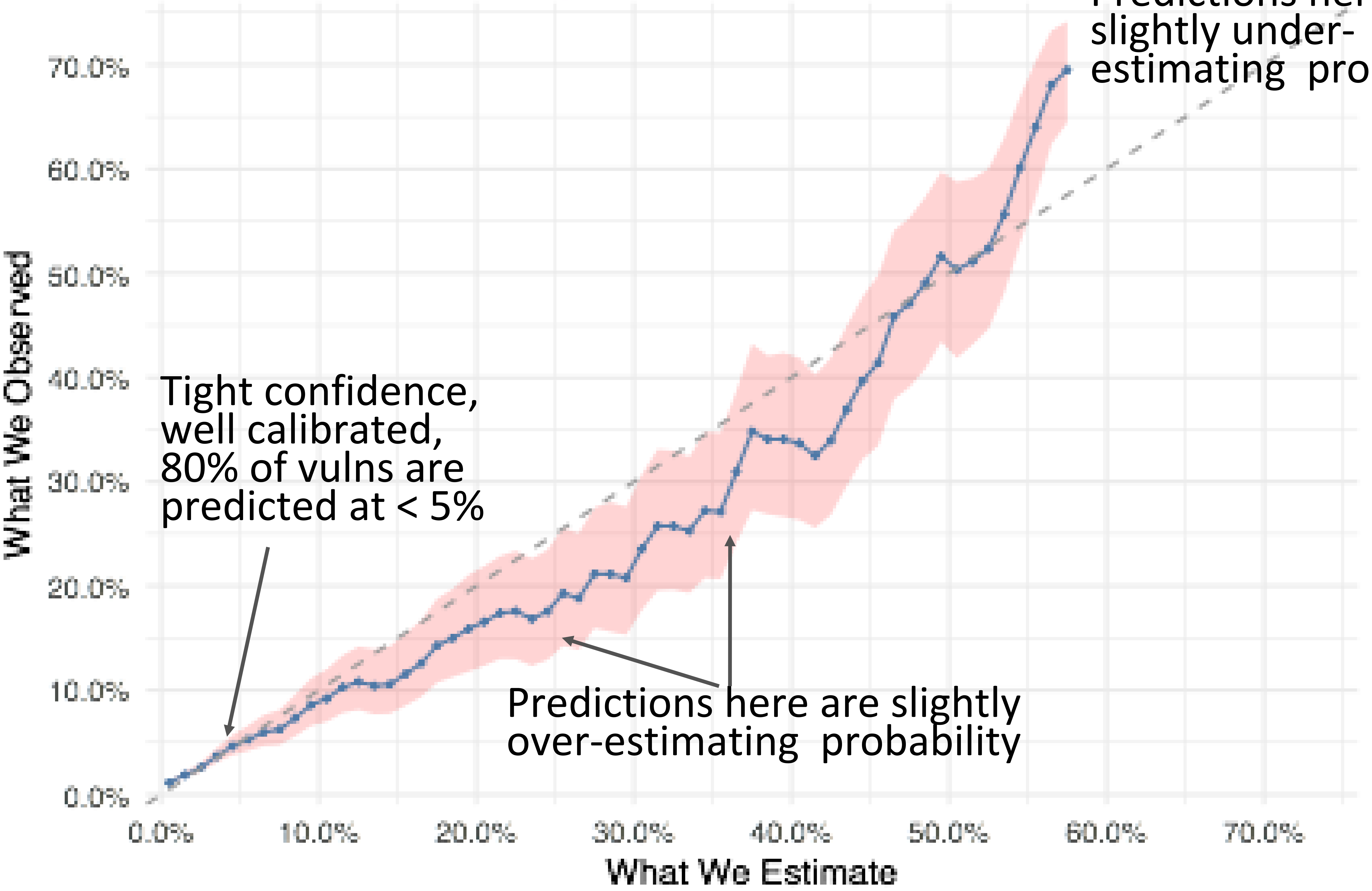
If there is a published exploit, in metasploit: 40% chance

...AND exploitDB published the exploit: 16%

What contributes to exploitation in the wild?



Predicting Probability: “well calibrated”



Predictions here are slightly under-estimating probability

Tight confidence, well calibrated, 80% of vulns are predicted at < 5%

Predictions here are slightly over-estimating probability

Apply What You Have Learned Today

- Next week you should:
  - Look at your own vulnerability efforts, what are you using beyond CVSS?
  - Investigate how you are tracking open and closed vulnerabilities.
- In the next month:
  - Start collecting exploit(ed) vulnerabilities from your own sensors.
- Within six months you should:
  - Calculate and track your own Coverage, Efficiency and Capacity
  - Compare your strategy to other prioritization strategies
  - Look for more research coming soon!

RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: HT-F03

The Etiology of Vulnerability Exploitation

Jay Jacobs

Data Scientist
Cyentia Institute
@jayjacobs

Michael Roytman

Chief Data Scientist
Kenna Security
@mroytman