RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: RMG2-R07

Measuring Vulnerability Remediation Strategies with Real-World Data

Wade Baker, PhD

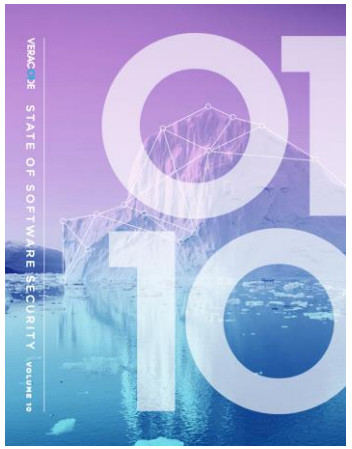
Partner, Cyentia Institute
Professor, Virginia Tech
@wadebaker

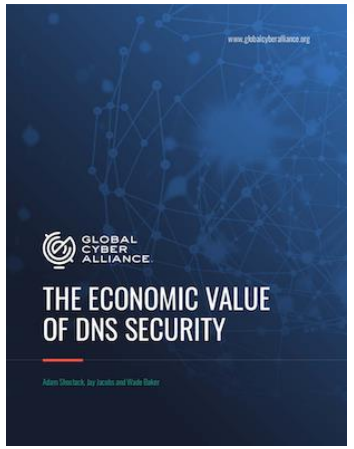
Benjamin Edwards, PhD

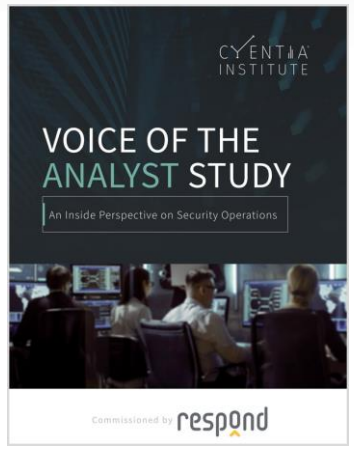
Senior Data Scientist
Cyentia Institute
@benjamesedwards

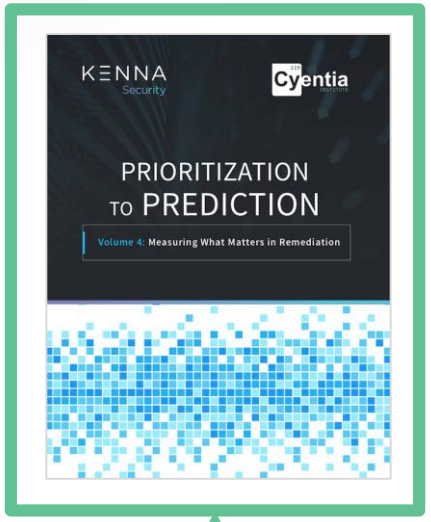
Data-driven cybersecurity research

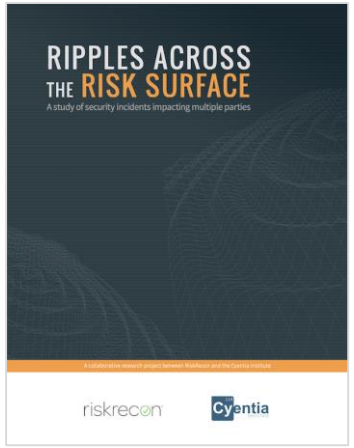
https://www.cyentia.com/research/

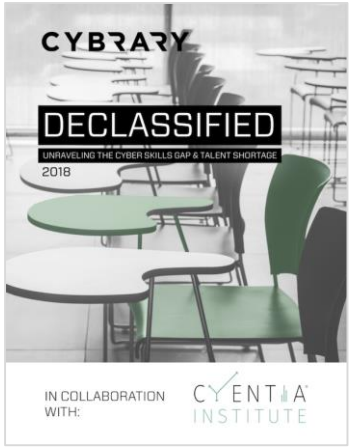


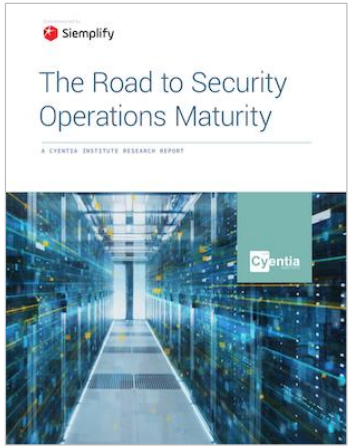












Our talk today comes from this research

Core questions for vulnerability remediation

Q: Can orgs remediate all vulnerabilities in their environment?

Q: Can organizations remediate vulnerabilities before exploitation?

Q: Can orgs remediate all high-risk vulns in their environment?

Q: What factors drive better/worse remediation performance?

Core questions for vulnerability remediation

Q: Can orgs remediate all vulnerabilities in their environment?

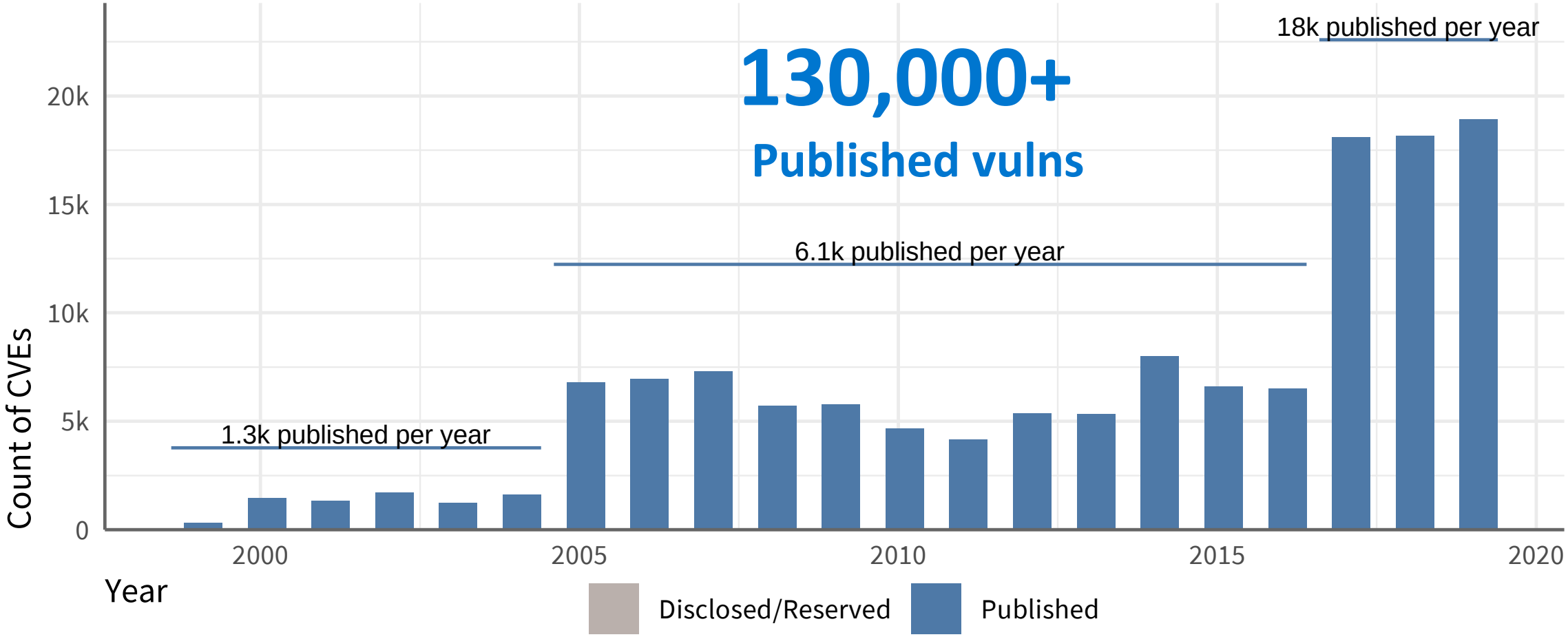
Q: Can organizations remediate vulnerabilities before exploitation?

Q: Can orgs remediate all high-risk vulns in their environment?

Q: What factors drive better/worse remediation performance?

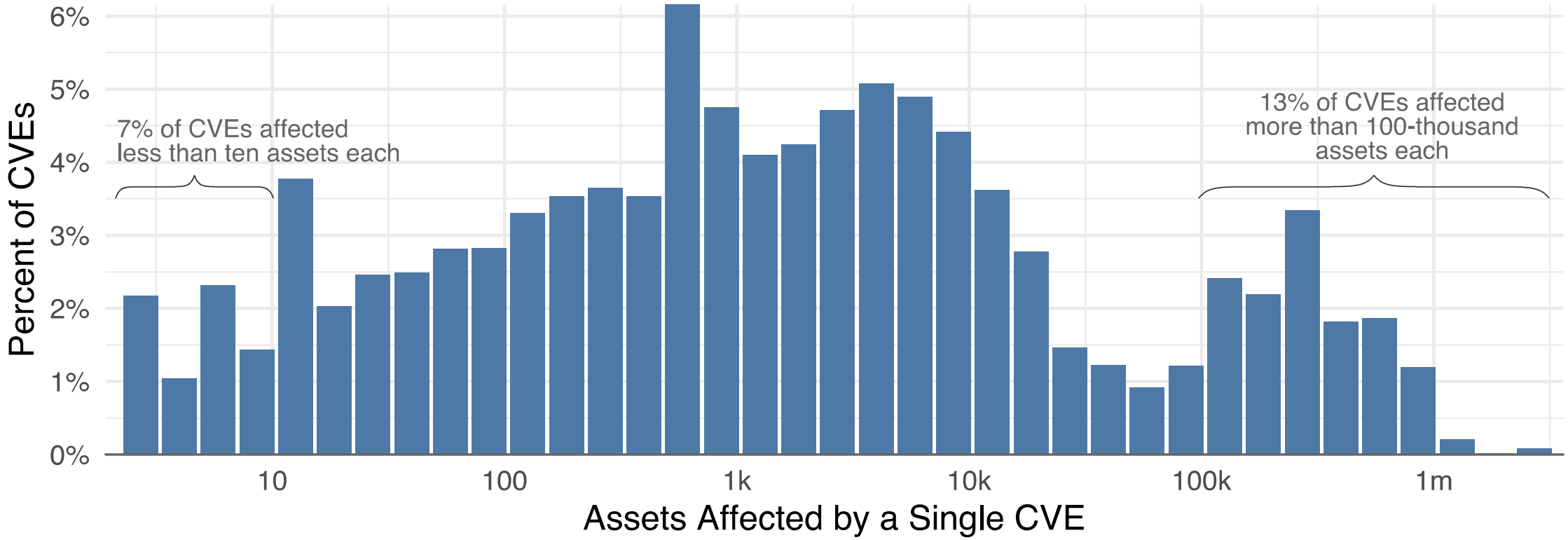
There are A LOT of vulnerabilities

Monthly volume of published CVEs from 1999 through 2019



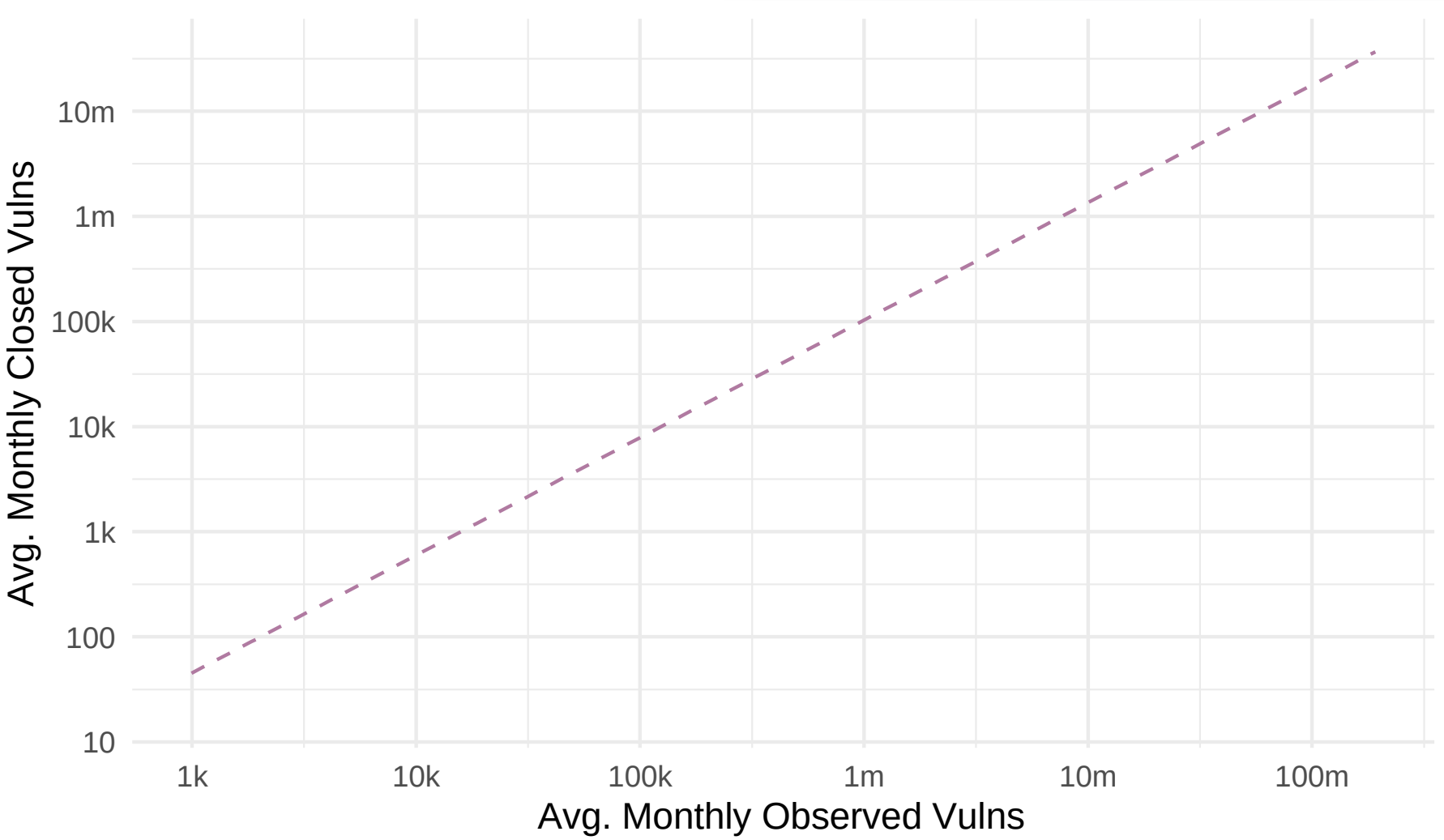
Scope of exposures can be large

Distribution of the total number of assets affected by CVEs



On average, firms fix 1 in 10 vulnerabilities

Comparison of average number of open and closed vulnerabilities per month



Core questions for vulnerability remediation

Q: Can orgs remediate all vulnerabilities in their environment?

A: Nope; not even close.

Q: Can organizations remediate vulnerabilities before exploitation?

Q: Can orgs remediate all high-risk vulns in their environment?

Q: What factors drive better/worse remediation performance?

Core questions for vulnerability remediation

Q: Can orgs remediate all vulnerabilities in their environment?

A: Nope; not even close.

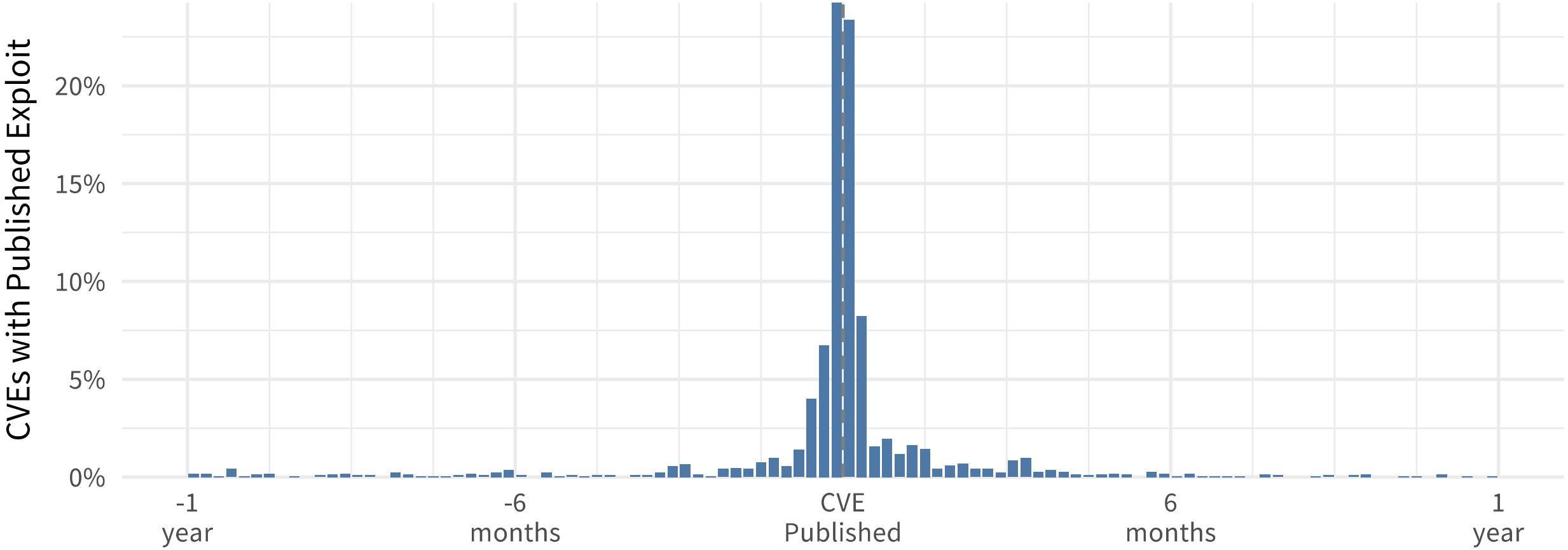
Q: Can organizations remediate vulnerabilities before exploitation?

Q: Can orgs remediate all high-risk vulns in their environment?

Q: What factors drive better/worse remediation performance?

Weaponization happens quickly

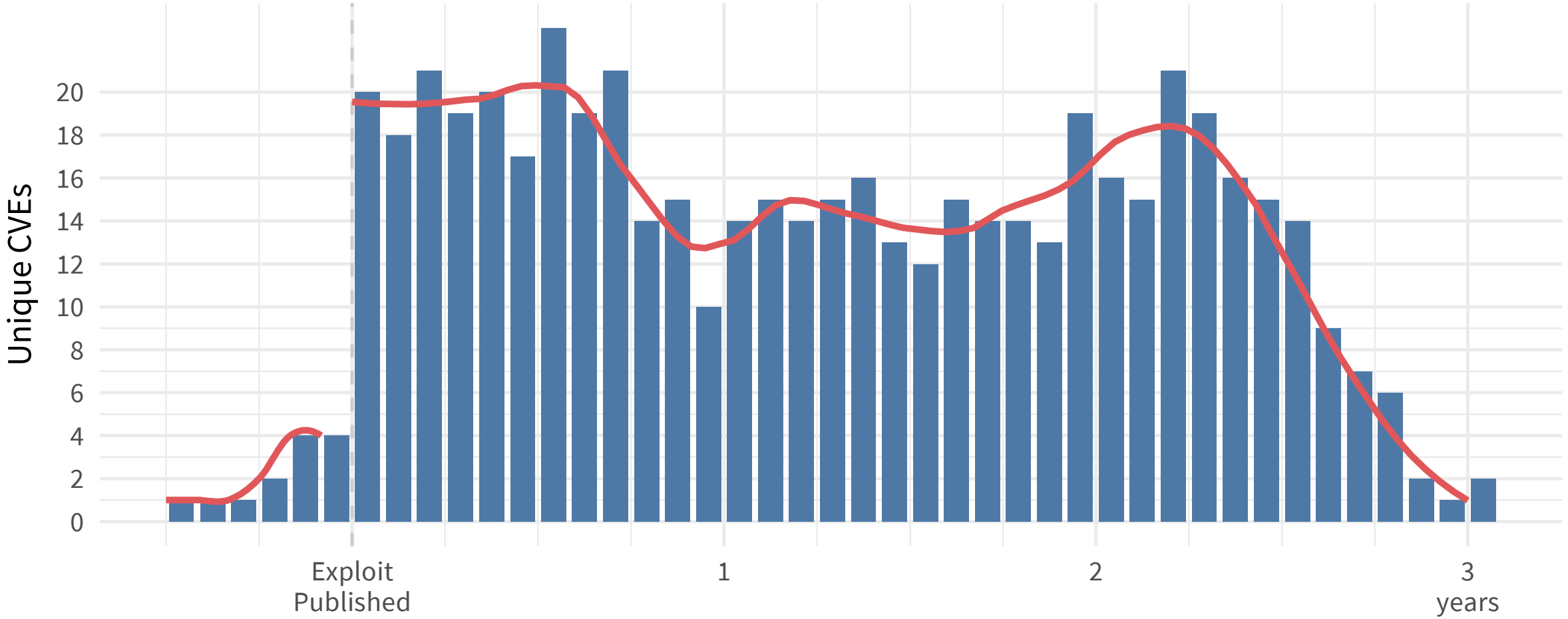
Exploit publication date relative to CVE publication date



Source: Kenna / Cyentia

Exploitation unfolds gradually

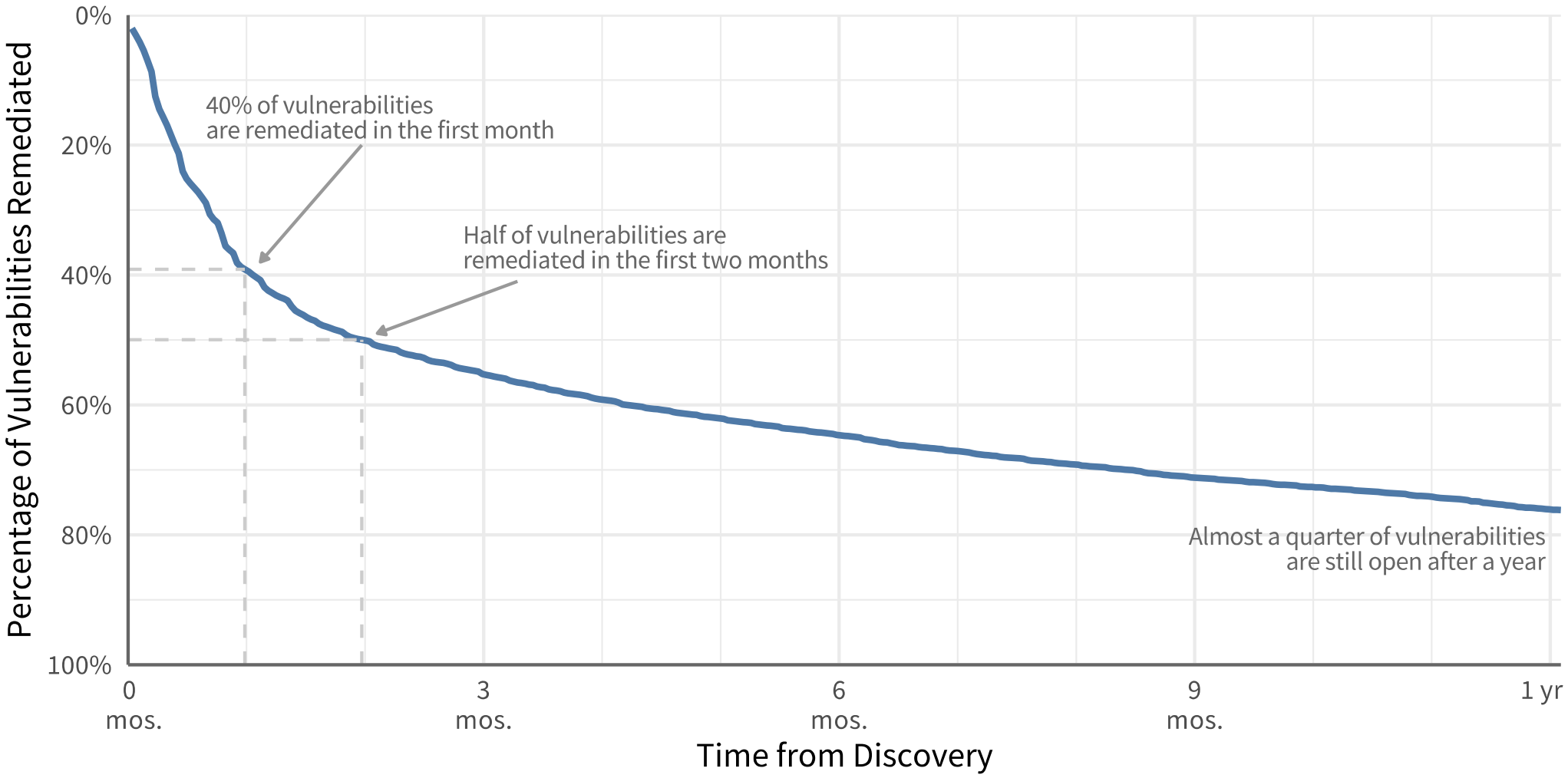
First detected exploitation relative to exploit publication date, by number of unique CVEs



Source: Kenna / Cyentia

Remediation takes time

Overall vulnerability survival analysis across firms



Core questions for vulnerability remediation

Q: Can orgs remediate all vulnerabilities in their environment?

A: Nope; not even close.

Q: Can organizations remediate vulnerabilities before exploitation?

A: Not before weaponization but maybe before you're exploited.

Q: Can orgs remediate all high-risk vulns in their environment?

Q: What factors drive better/worse remediation performance?

Core questions for vulnerability remediation

Q: Can orgs remediate all vulnerabilities in their environment?

A: Nope; not even close.

Q: Can organizations remediate vulnerabilities before exploitation?

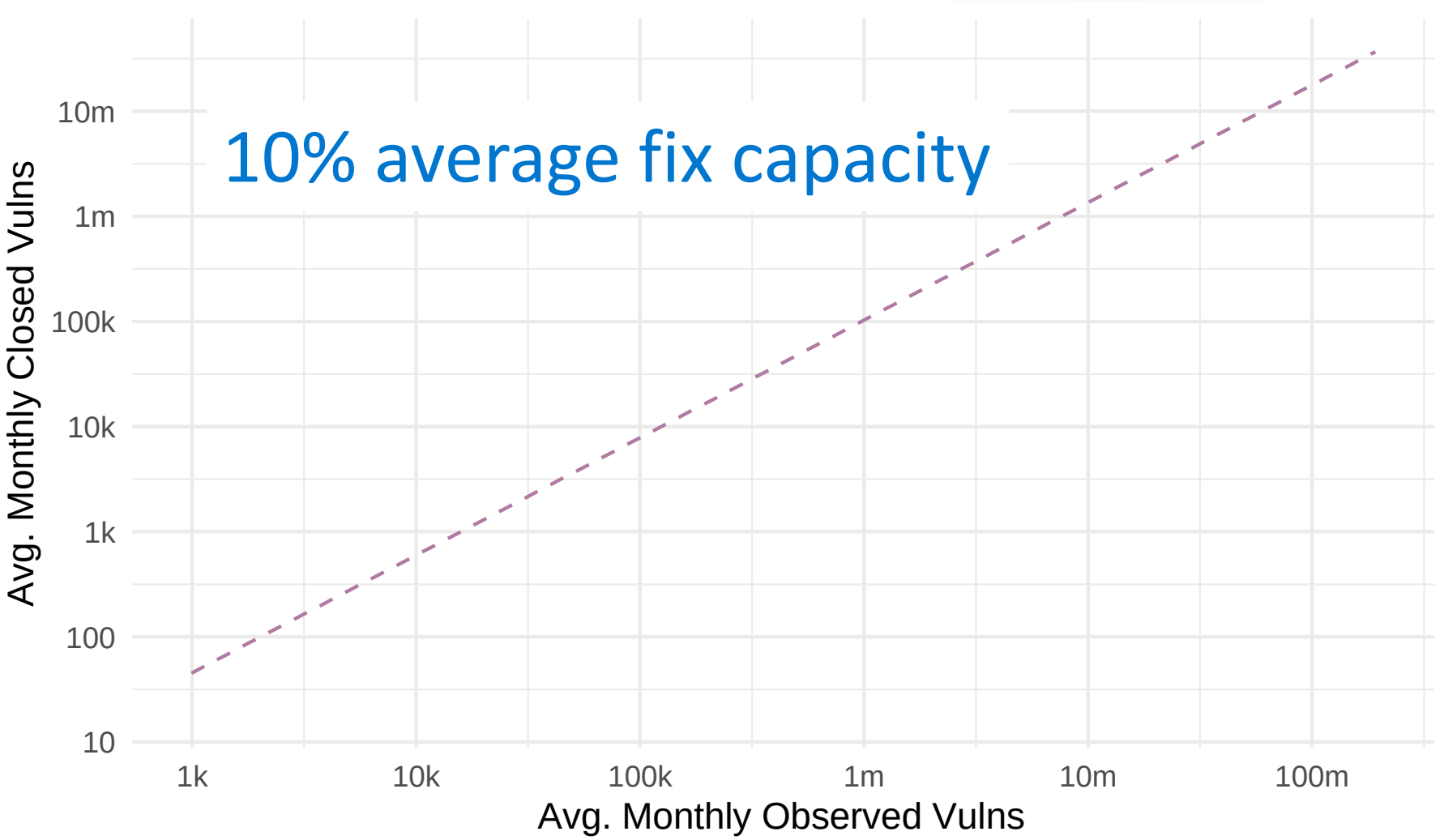
A: Not before weaponization but maybe before you're exploited.

Q: Can orgs remediate all high-risk vulns in their environment?

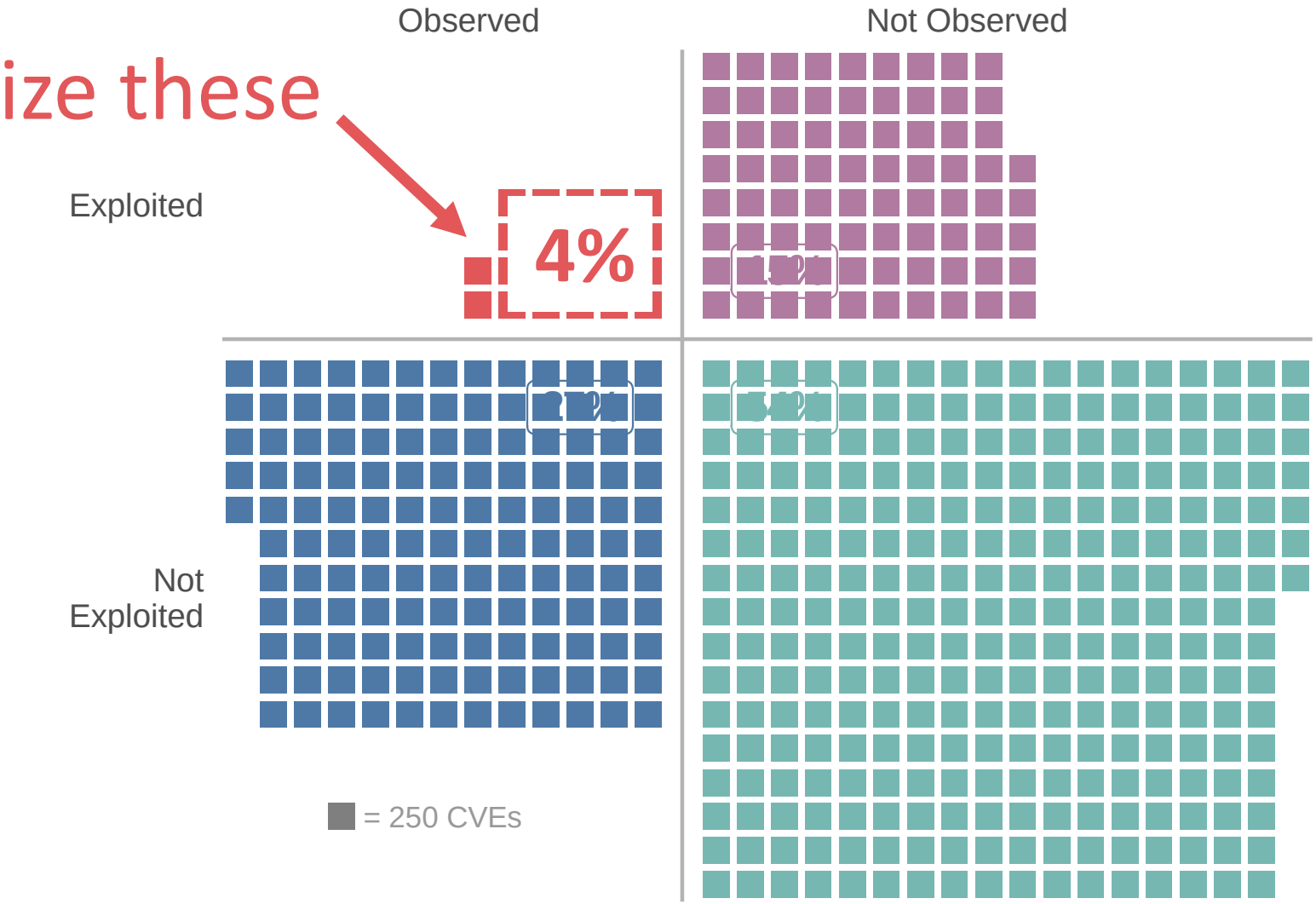
Q: What factors drive better/worse remediation performance?

REVIEW: Firms can't fix all vulnerabilities

Comparison of average number of open and closed vulnerabilities per month

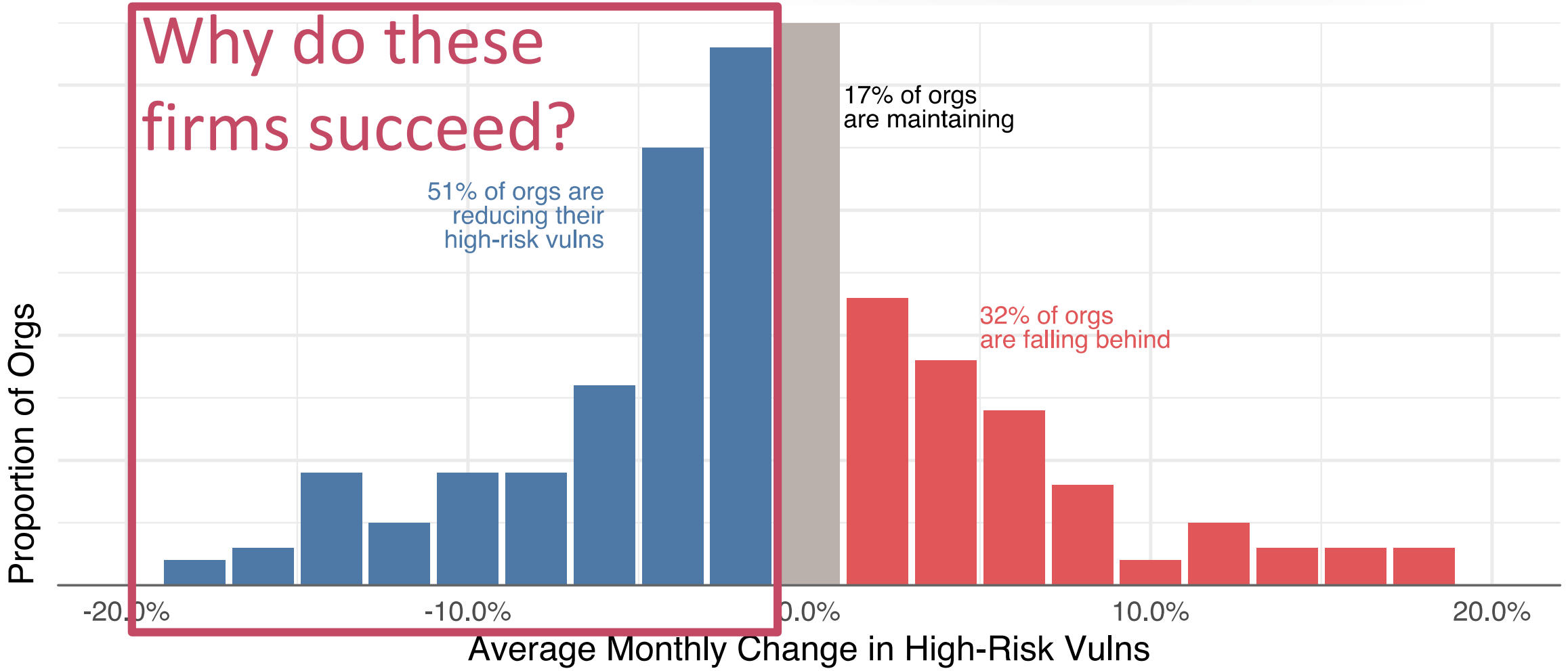


Maybe “ALL” vulns isn’t the best measure of success



2 in 3 firms successfully remediate high-risk vulns

Comparison of net remediation capacity for known-exploited vulnerabilities among firms



Core questions for vulnerability remediation

Q: Can orgs remediate all vulnerabilities in their environment?

A: Nope; not even close.

Q: Can organizations remediate vulnerabilities before exploitation?

A: Not before weaponization but maybe before you're exploited.

Q: Can orgs remediate all high-risk vulns in their environment?

A: Yes! Some pay down vuln debt with better focus and execution.

Q: What factors drive better/worse remediation performance?

Core questions for vulnerability remediation

Q: Can orgs remediate all vulnerabilities in their environment?

A: Nope; not even close.

Q: Can organizations remediate vulnerabilities before exploitation?

A: Not before weaponization but maybe before you're exploited.

Q: Can orgs remediate all high-risk vulns in their environment?

A: Yes! Some pay down vuln debt with better focus and execution.

Q: What factors drive better/worse remediation performance?

How do we measure “better” or “worse” performance?

- **Coverage**: Completeness of remediation. What percentage of exploited or “high-risk” vulnerabilities are remediated?
- **Efficiency**: Precision of remediation. What percentage of remediated vulnerabilities are actually high-risk?
- **Velocity**: Speed and progress of remediation.
- **Capacity**: Number of vulnerabilities that can be remediated in a given timeframe and net gain or loss.
- **Overall**: Composite performance measure based on the above.

Core questions for vulnerability remediation

Q: Can orgs remediate all vulnerabilities in their environment?

A: Nope; not even close.

Q: Can organizations remediate vulnerabilities before exploitation?

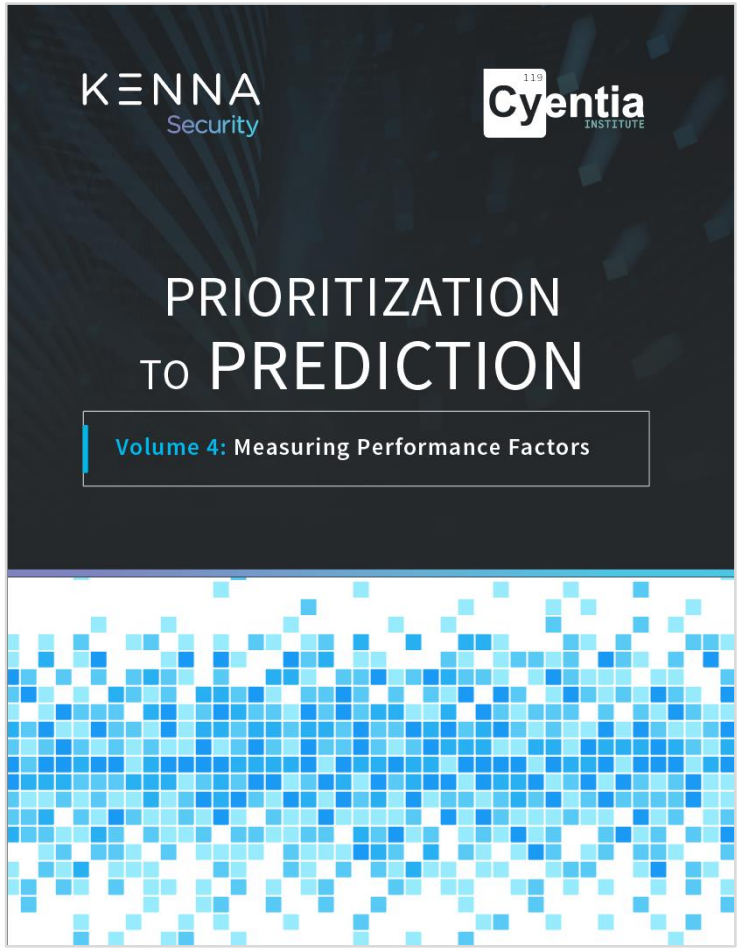
A: Not before weaponization but maybe before you're exploited.

Q: Can orgs remediate all high-risk vulns in their environment?

A: Yes! Some pay down vuln debt with better focus and execution.

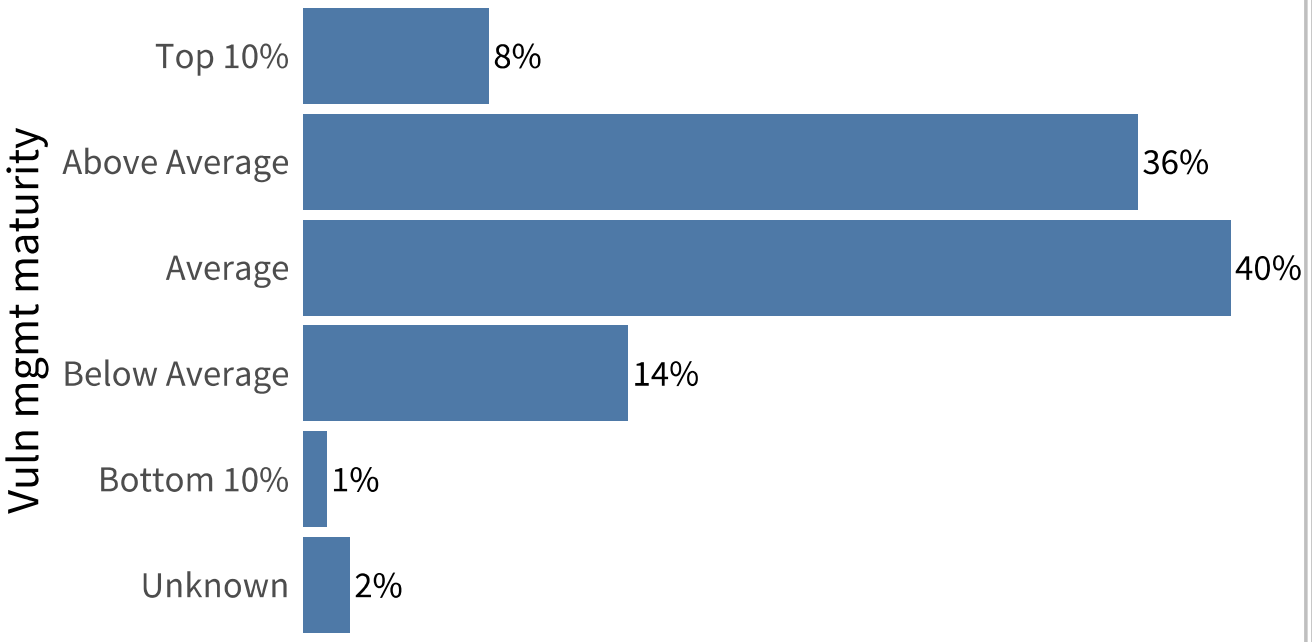
Q: What factors drive better/worse remediation performance?

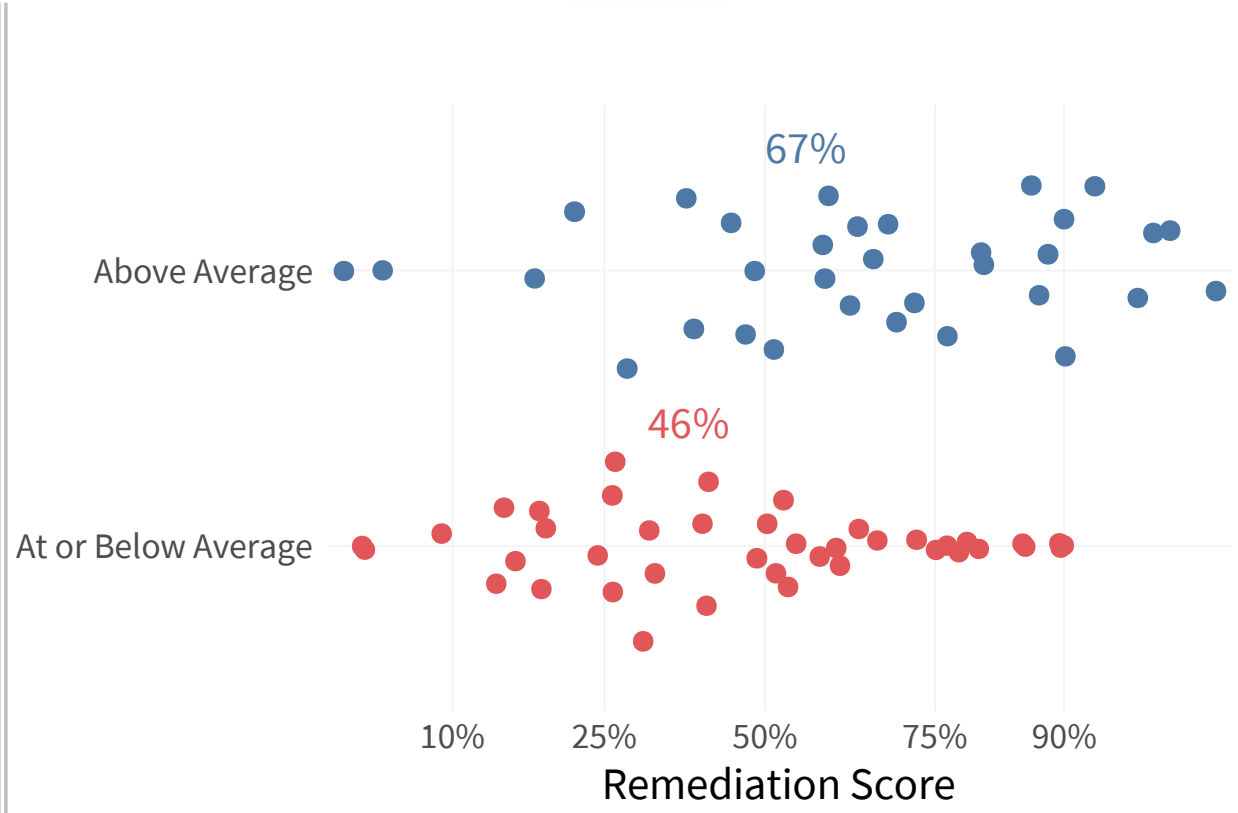
Identifying performance factors



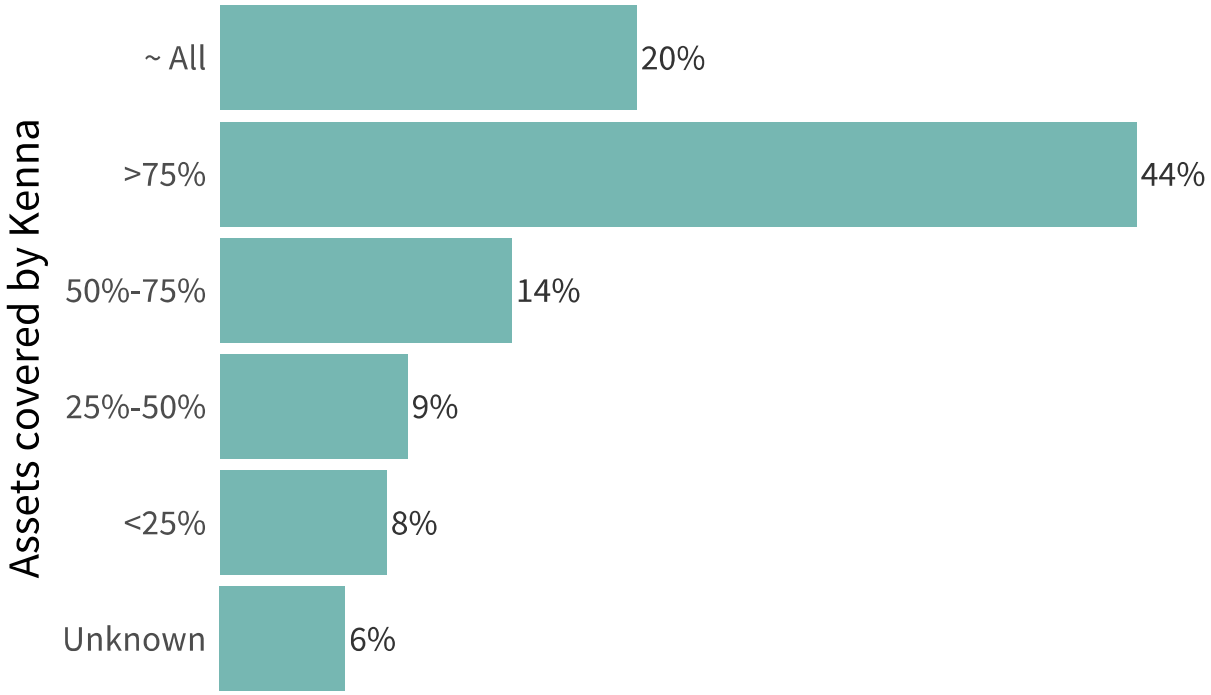
"We combine survey and observational data to test how internal VM program factors affect actual remediation performance measures."

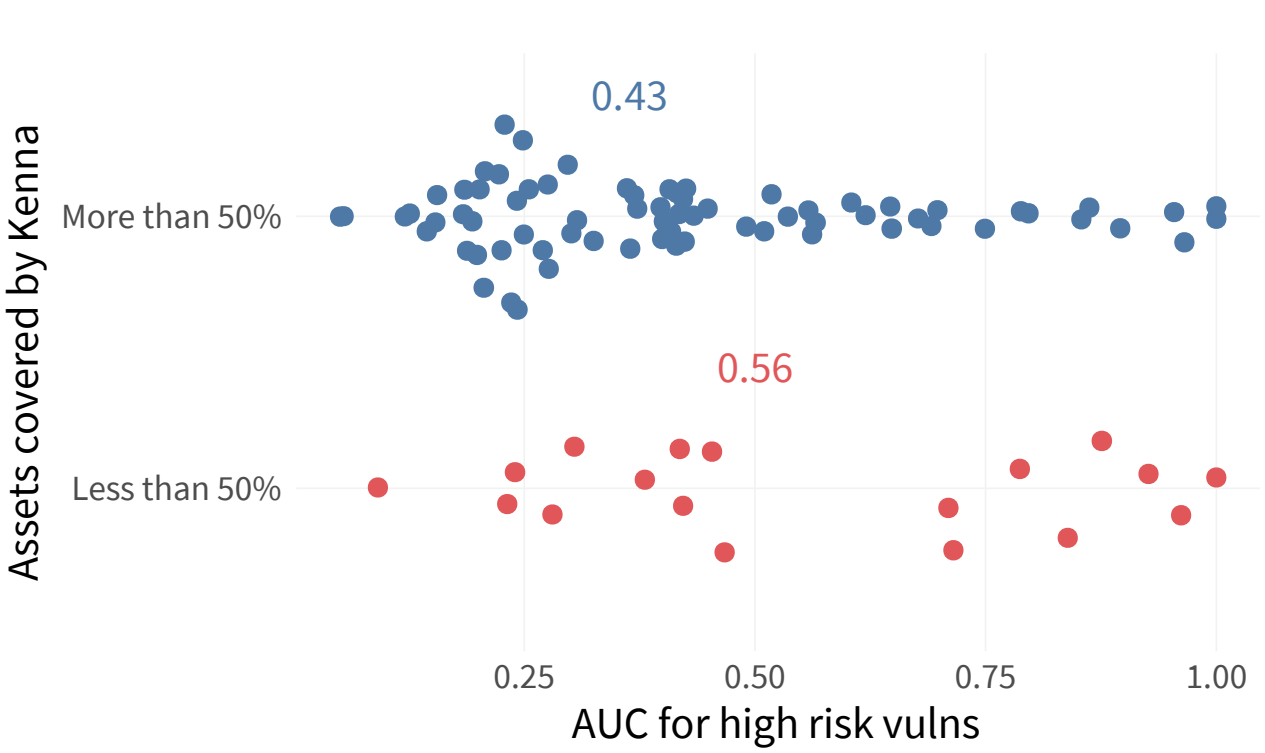
Overall VM maturity



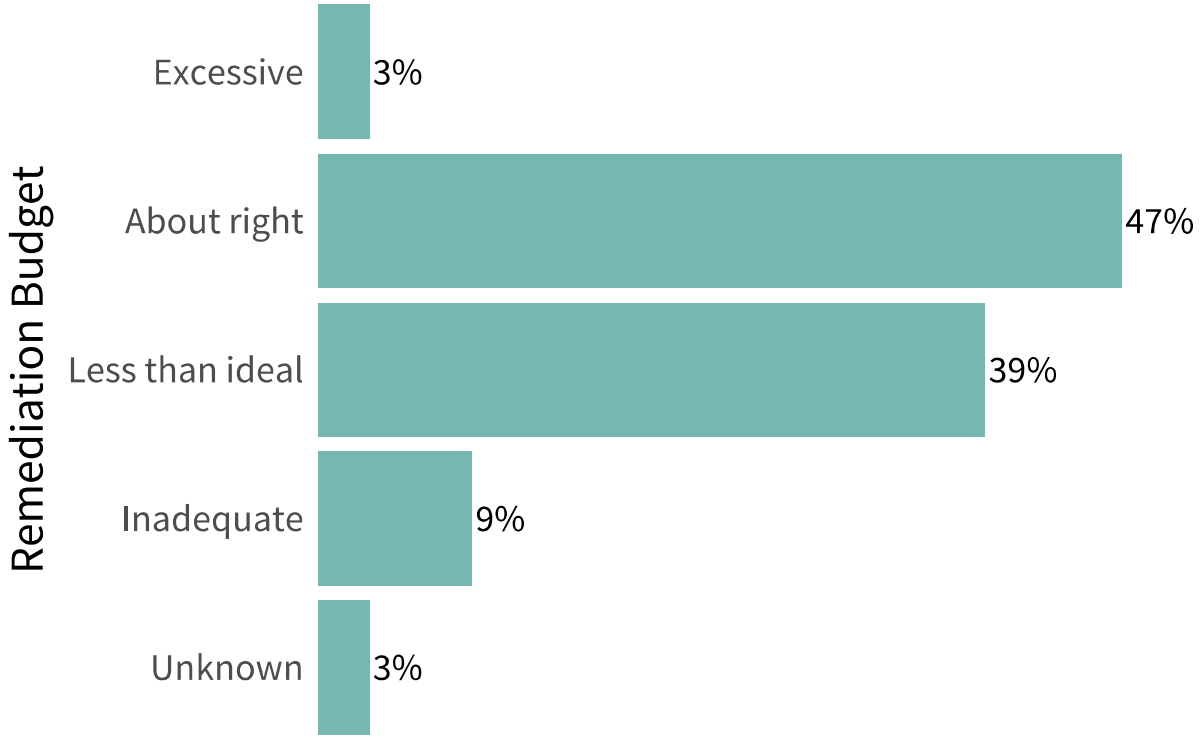


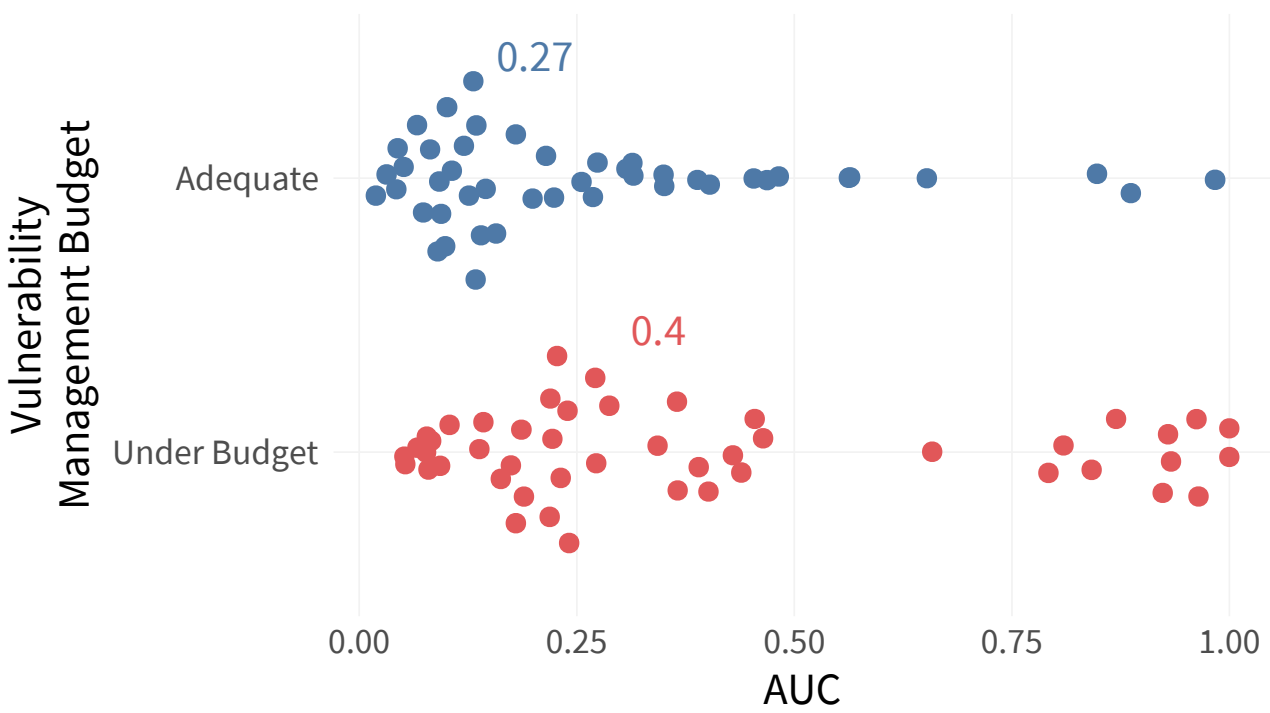
Assets under management



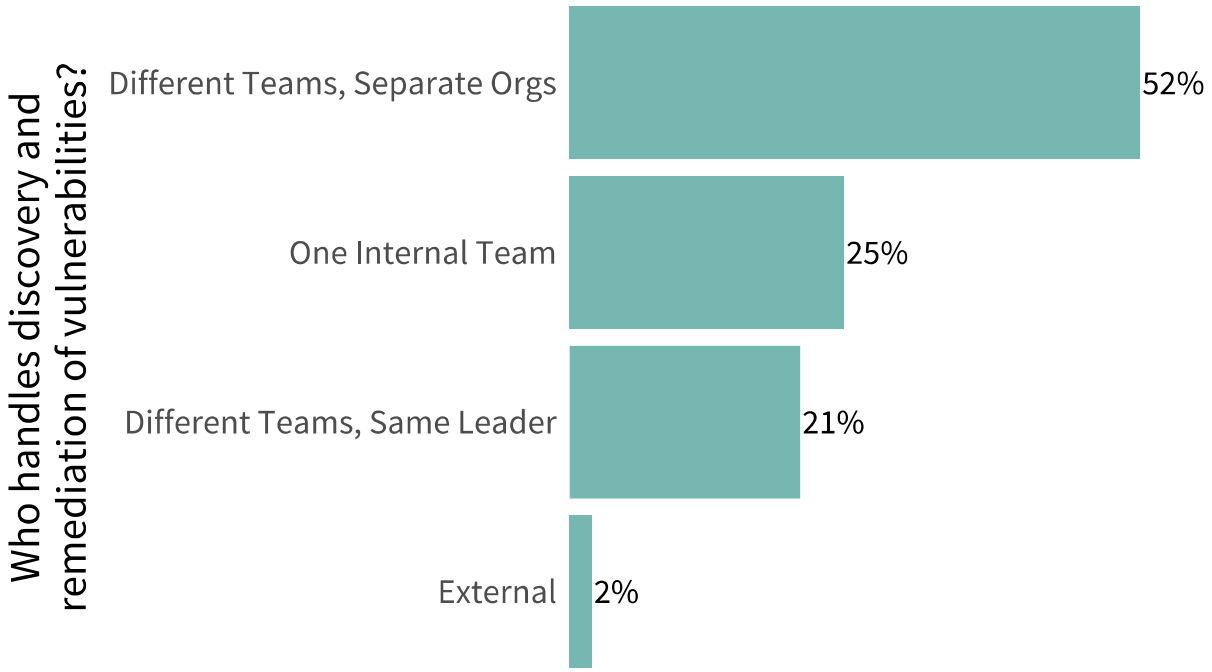


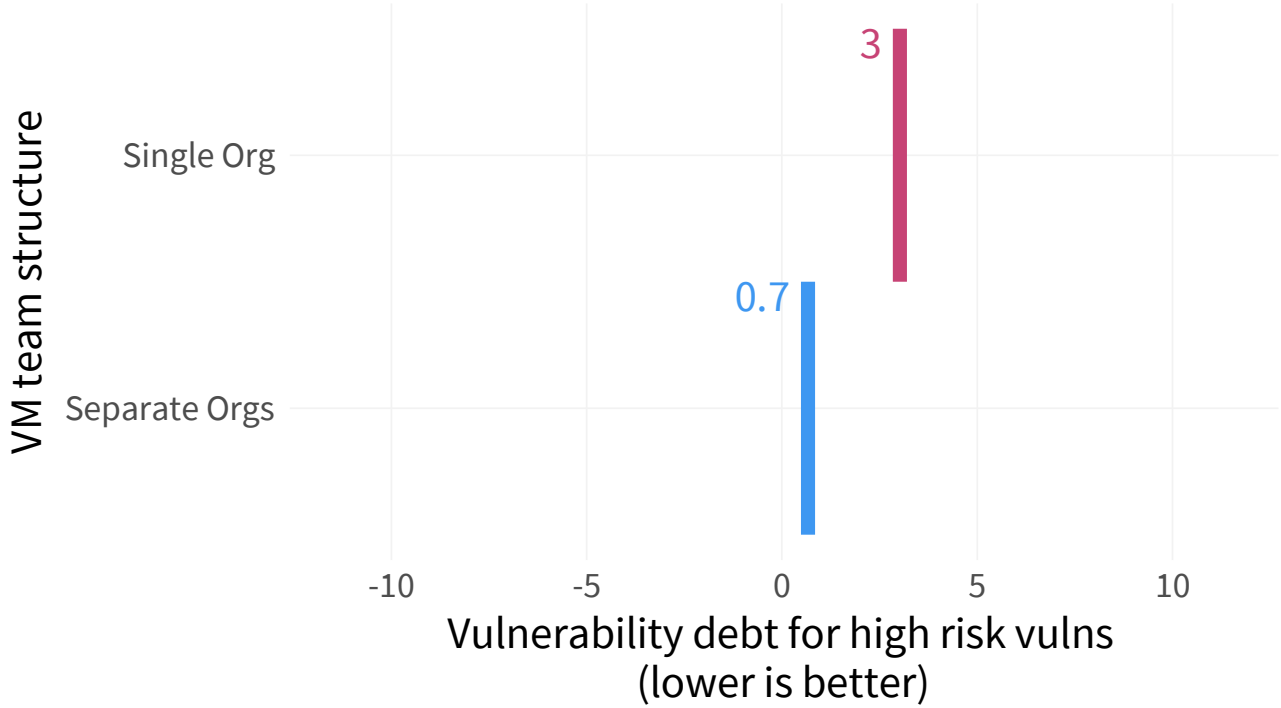
VM program budget



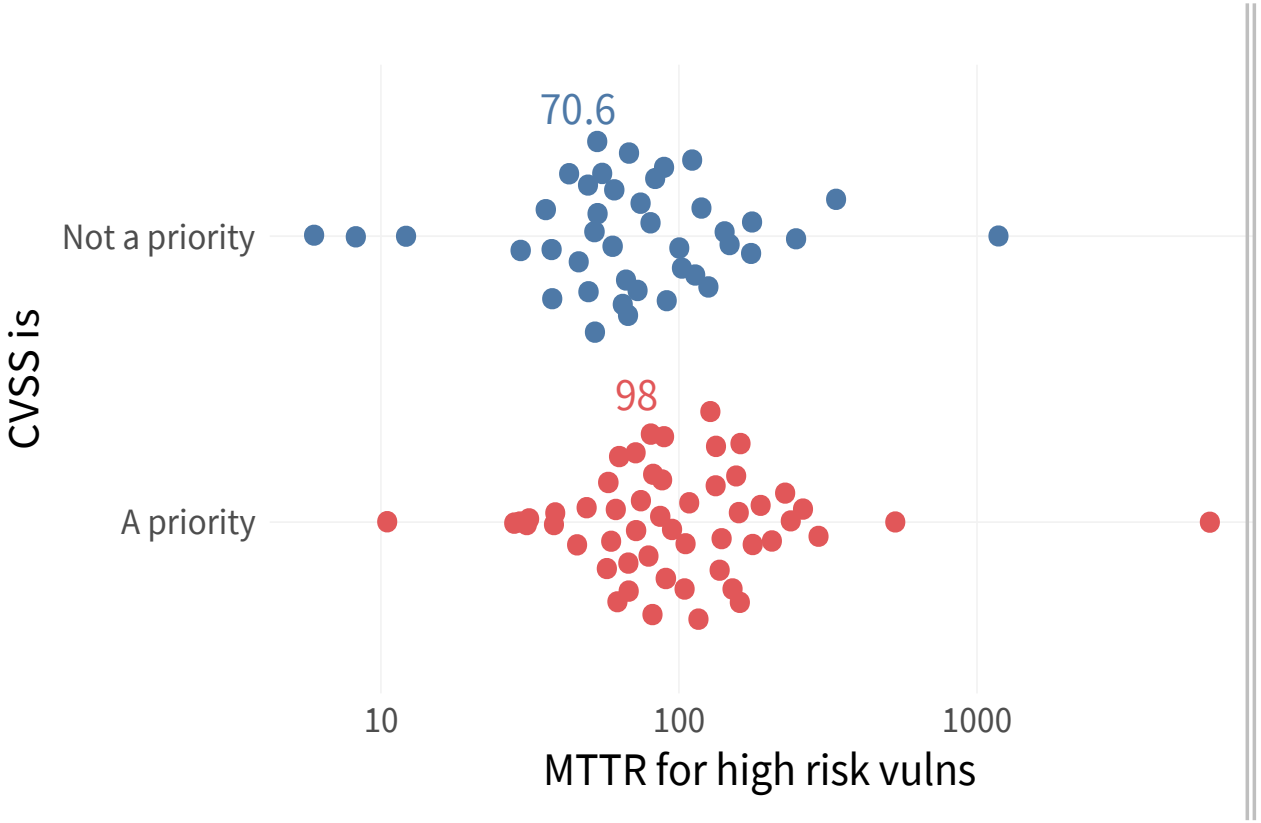


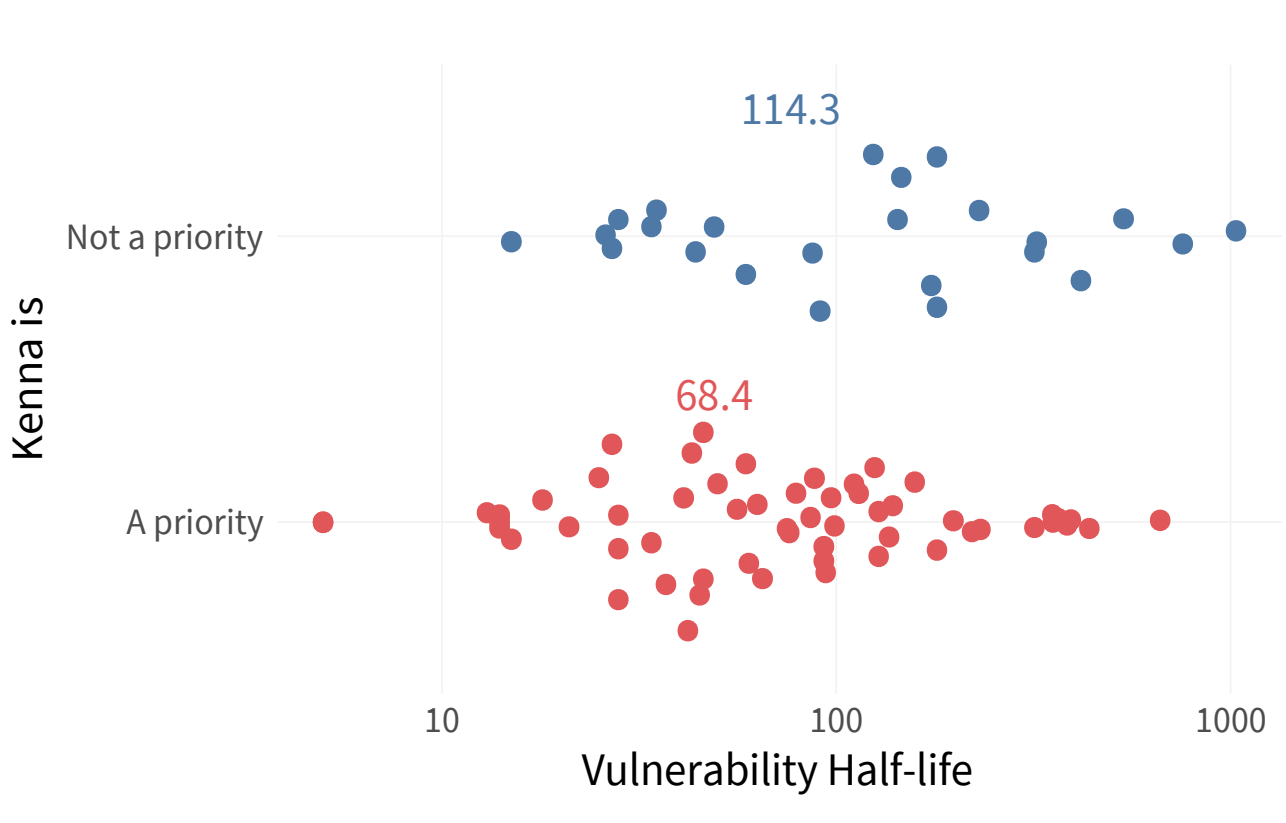
VM team structure





Prioritization criteria





CVSS is an objectively poor predictor of exploitation

Better coverage, but...

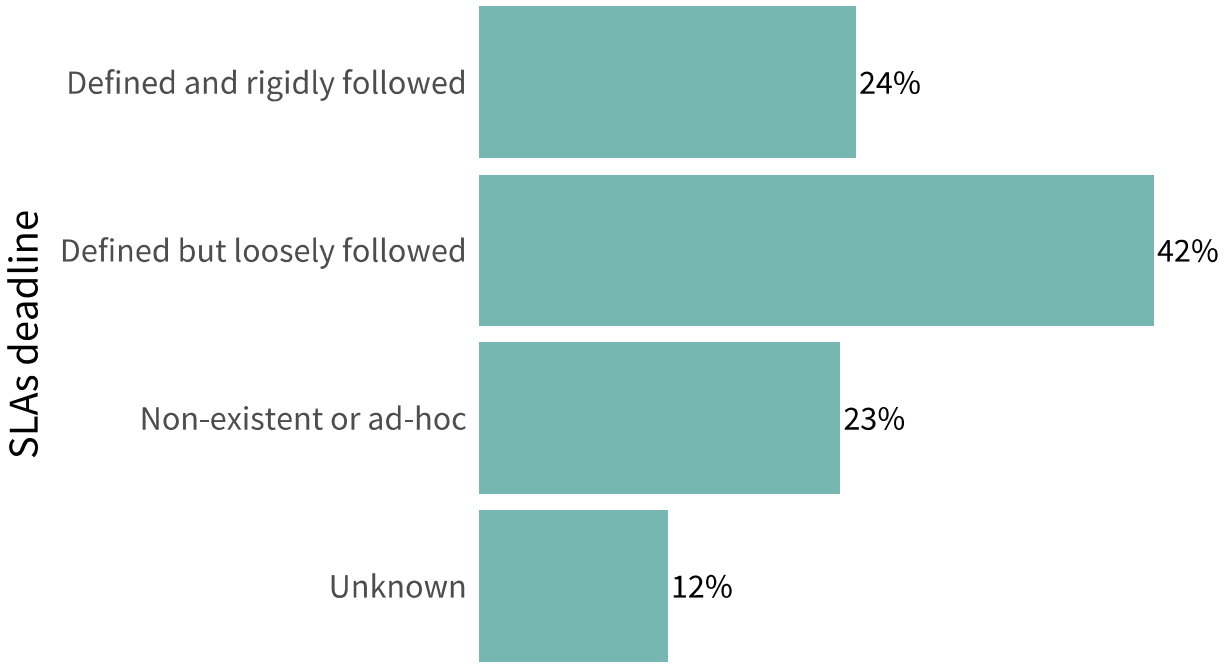
Wasted effort is high

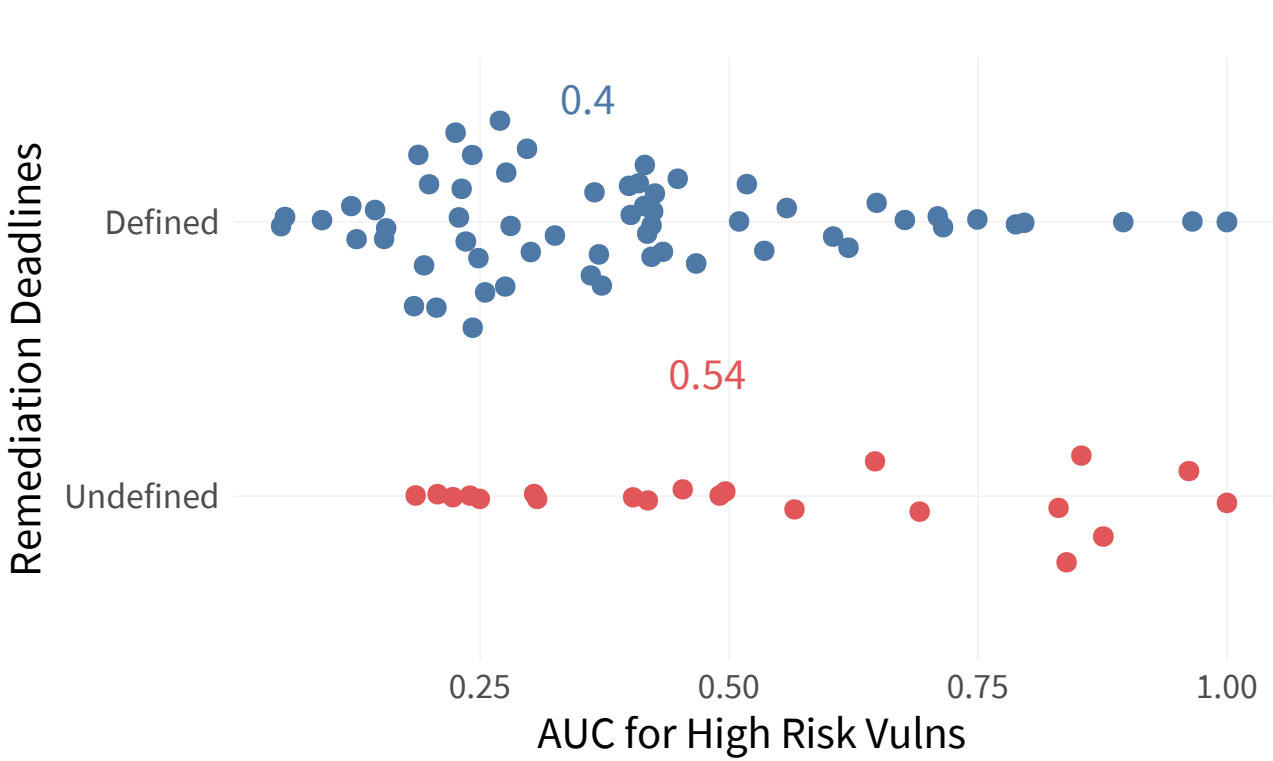
Remediate above CVSS Base Score

	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%

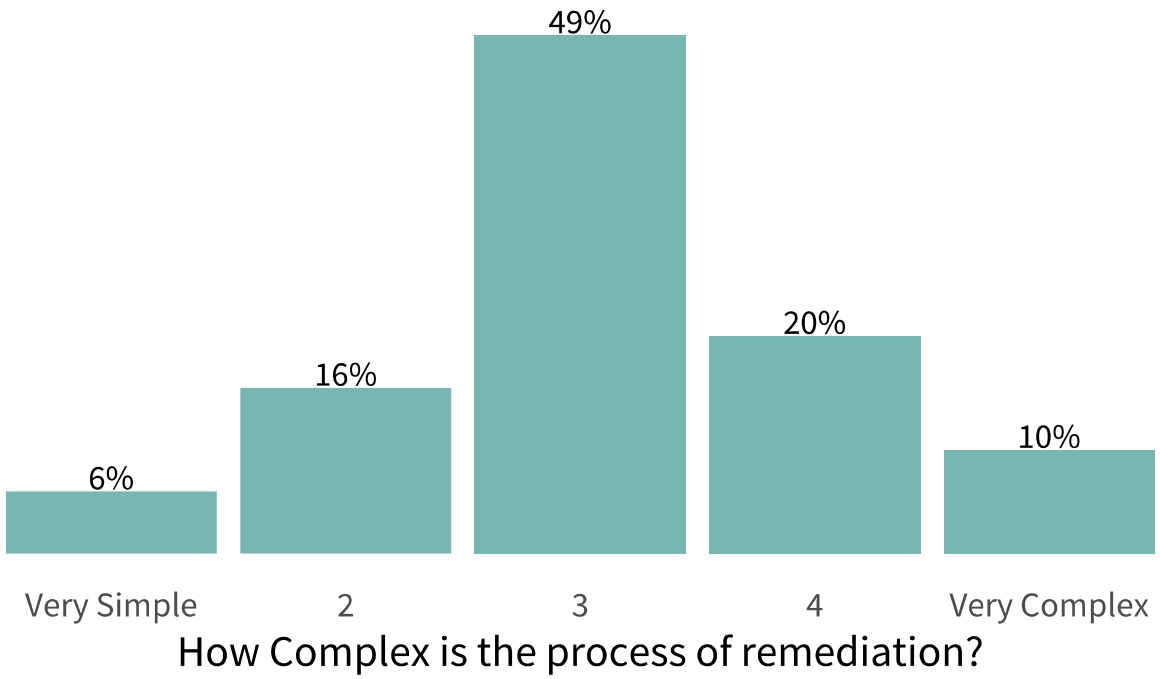
Source: Kenna / Cyentia

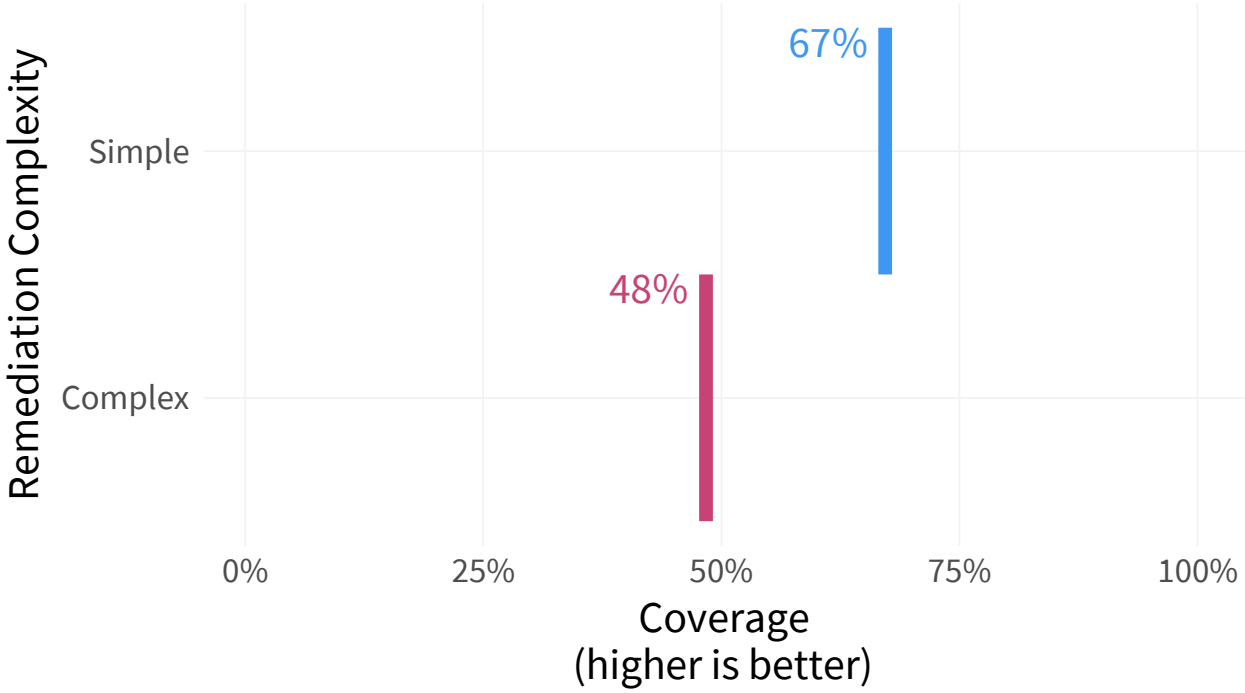
Remediation deadlines



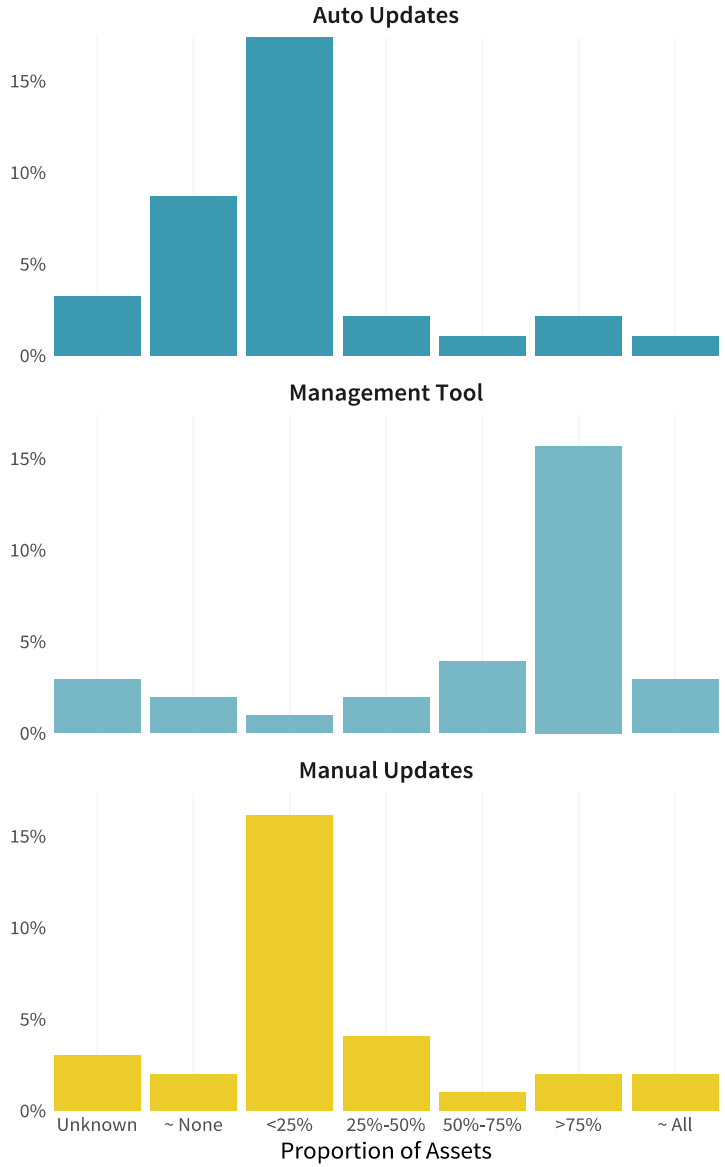


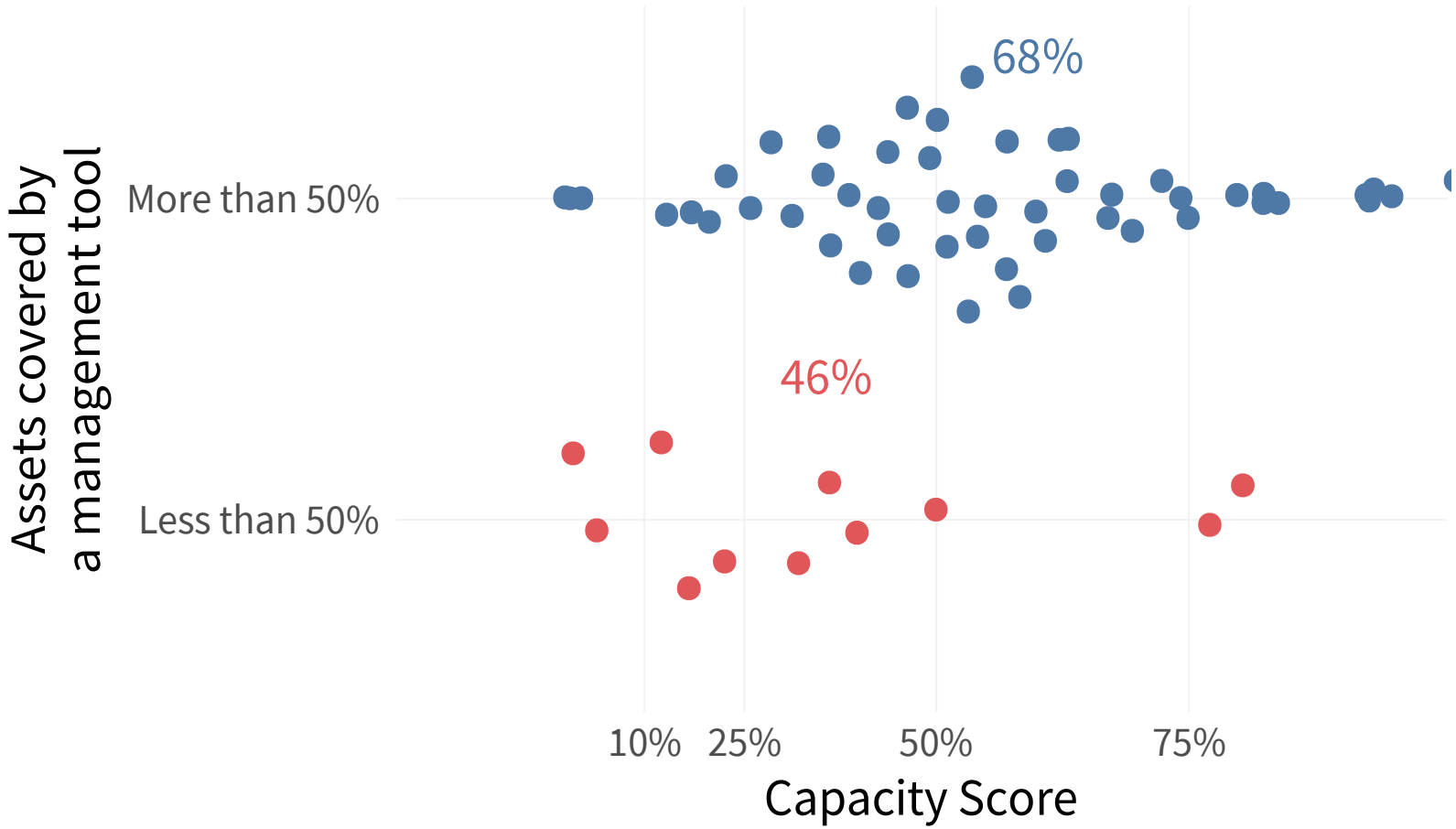
Process complexity





Patch deployment methods





Core questions for vulnerability remediation

Q: Can orgs remediate all vulnerabilities in their environment?

A: Nope; not even close.

Q: Can organizations remediate vulnerabilities before exploitation?

A: Not before weaponization but maybe before you're exploited.

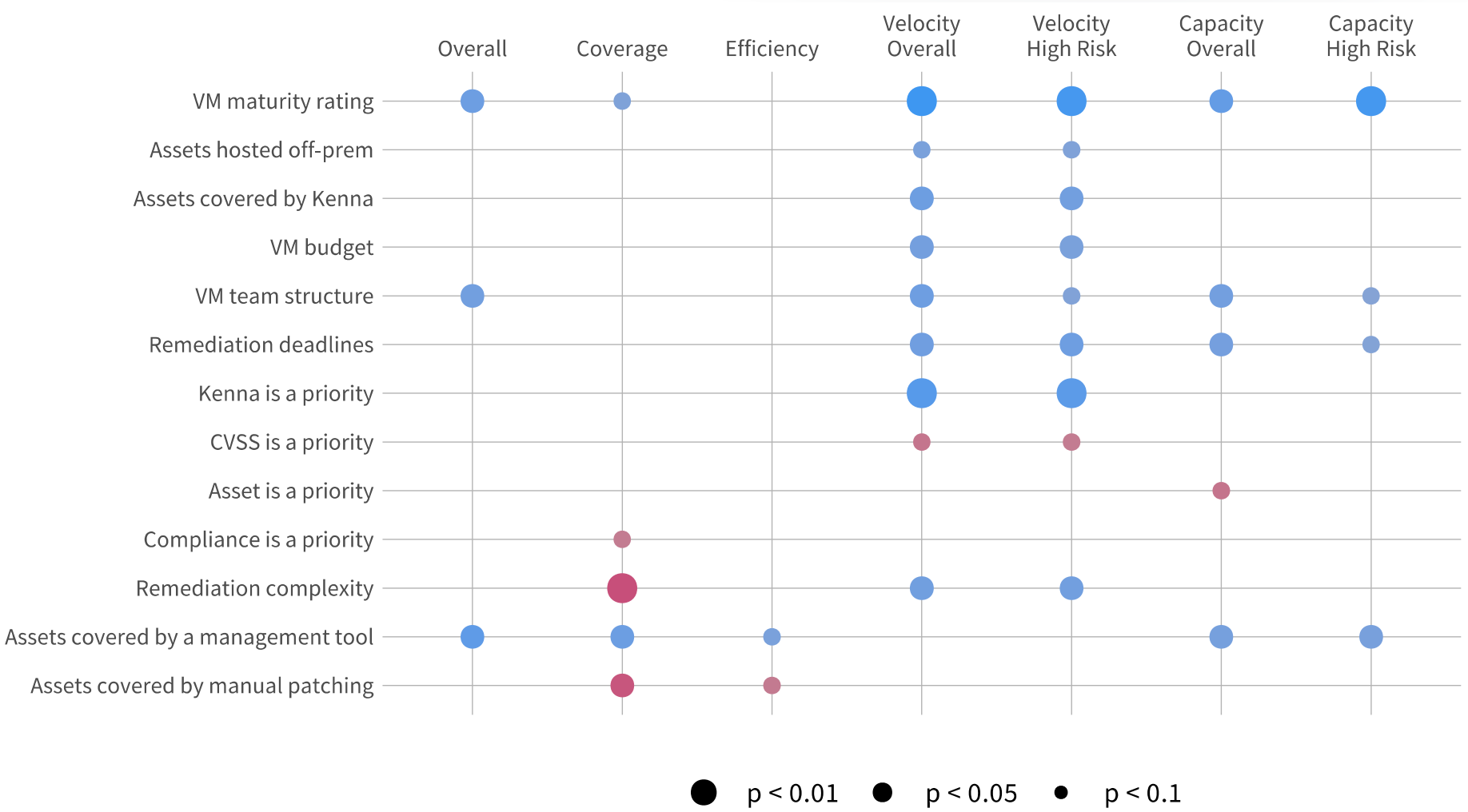
Q: Can orgs remediate all high-risk vulns in their environment?

A: Yes! Some pay down vuln debt with better focus and execution.

Q: What factors drive better/worse remediation performance?

A: Lots of them. Let's recap.

Summary of performance factors



RSAConference2020

So What?

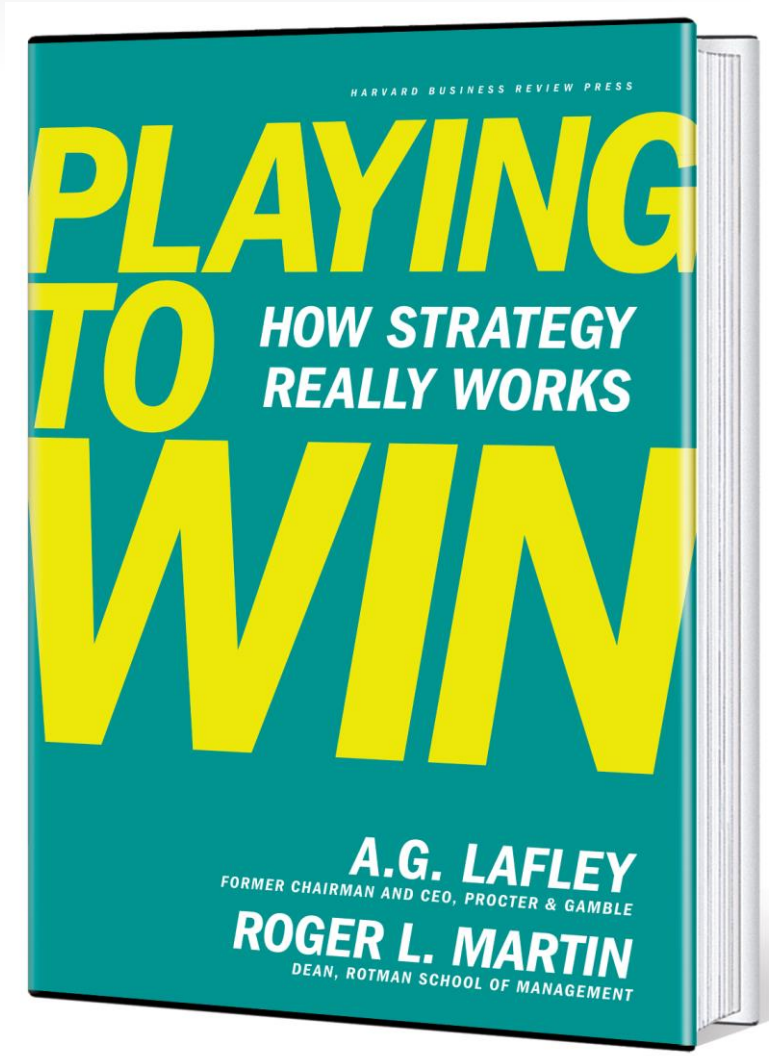
What should I take away from this talk?

Strategy makes a huge difference

The difference between ‘gaining ground’ and ‘falling behind’ in vulnerability remediation comes down to strategy.

What do you mean by strategy?

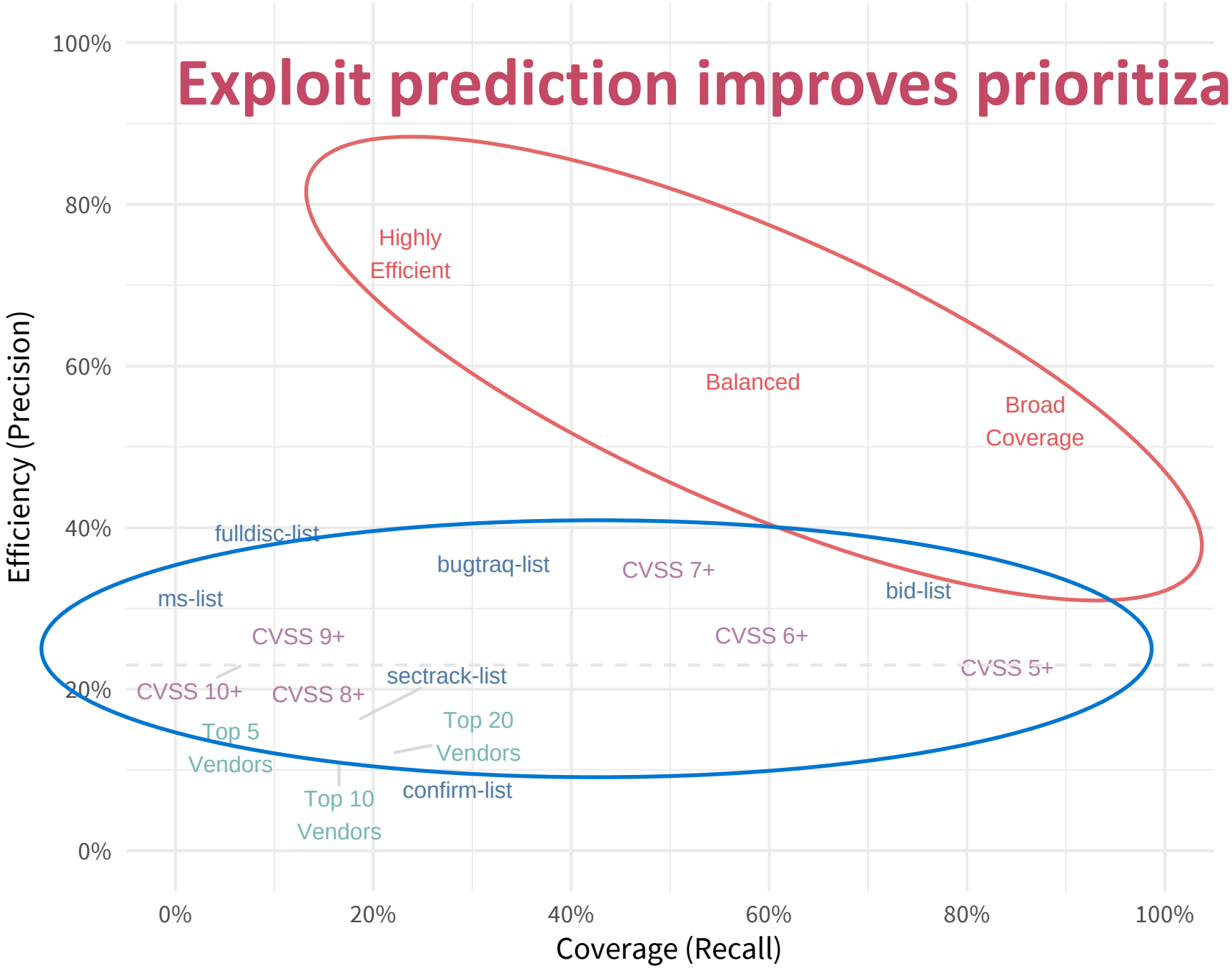
"Strategy is an integrated set of choices that uniquely positions the firm to create sustainable advantage"



Strategic choices in vulnerability remediation

- Which performance **measures** matter most to us?
- Which vulnerabilities should we **prioritize** for remediation?
- How do we **execute** remediation most effectively?
- How do we **organize** and govern for effective execution?

Exploit prediction improves prioritization



Source: Kenna / Cyentia

"Compared to a strategy fixing all CVEs with a CVSS of 7 or more, our model achieves **2X the efficiency** (61% vs 31%), **half the effort** (19K vs 37K CVEs), **1/3 false positives** (7K vs 25K CVEs), and **better coverage** (62% vs 53%)."

Additional resources for prioritizing vulnerabilities

- Workshop on the Economics of InfoSec (WEIS) paper:
  - https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_53.pdf
- Exploit Prediction Scoring System (EPSS) paper:
  - https://arxiv.org/abs/1908.04856
- Online EPSS calculator:
  - https://www.kennaresearch.com/tools/epss-calculator/