Carnegie Mellon University
HeinzCollege
INFORMATION SYSTEMS • PUBLIC POLICY • MANAGEMENT

Capital One
Exploitability Score

FINAL PRESENTATION

APRIL 25, 2023

Agenda

1. Introductions
2. Problem Space
3. Quick Review
4. Research & Recommendations
5. Future Work

Agenda

1. **Introductions**
2. Problem Space
3. Quick Review
4. Research & Recommendations
5. Future Work

Our Client

Capital One is a diversified financial services company headquartered in McLean, Virginia, United States. The company offers a broad range of financial products and services to consumers, small businesses, and commercial clients in the United States, Canada, and the United Kingdom.

Agenda

1. Introductions
2. **Problem Space**
3. Quick Review
4. Research & Recommendations
5. Future Work

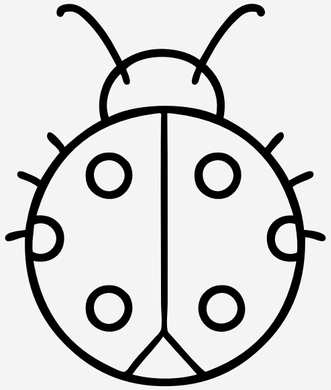
Background Problem

Cyber Attacks

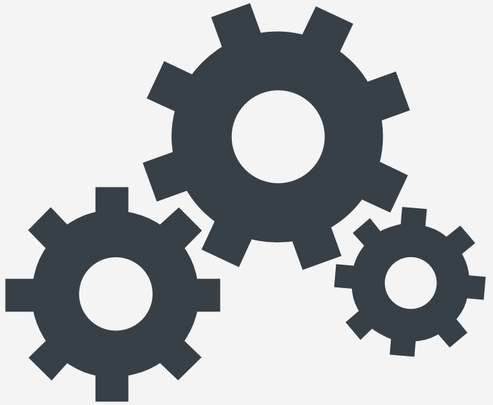
Banking sector was the target of **17%** of all cyber attacks in 2020, making it the **second** most targeted industry after the IT sector.

https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf

2 Problem Space



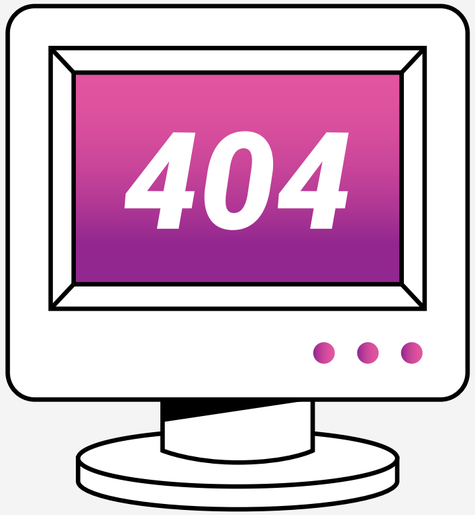
Software Bugs



Misconfigurations

Causes

Malicious Attacks



Human Error

https://codesigningstore.com/common-software-vulnerabilities

Problem Statement

2 Problem Space

CVSS+

Need for a more effective score system that prioritizes vulnerabilities based on their exploitability, in addition to their severity and impact.

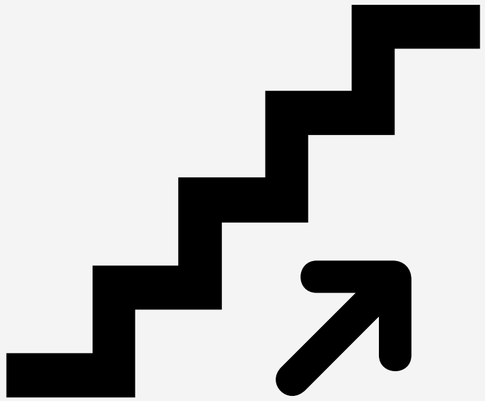
Exploitability

Cost

Financial Cost

Vulcan Cyber:
For Medium-to-large enterprises

$1,600,000-
Detection & Remediation & Reporting



$1,350,000 -
Detection & Remediation

- https://l.vulcancyber.com/hubfs/Ebooks%20and%20White%20Papers/The%20Business%20Case%20for%20Vulnerability%20Remediation%20Automation.pdf

Timing Cost

For one vulnerability -

- Average 16 minutes to detect
- Average longer than 16 minutes to prioritize
- Average longer than 21 minutes to remediate

More than an hour

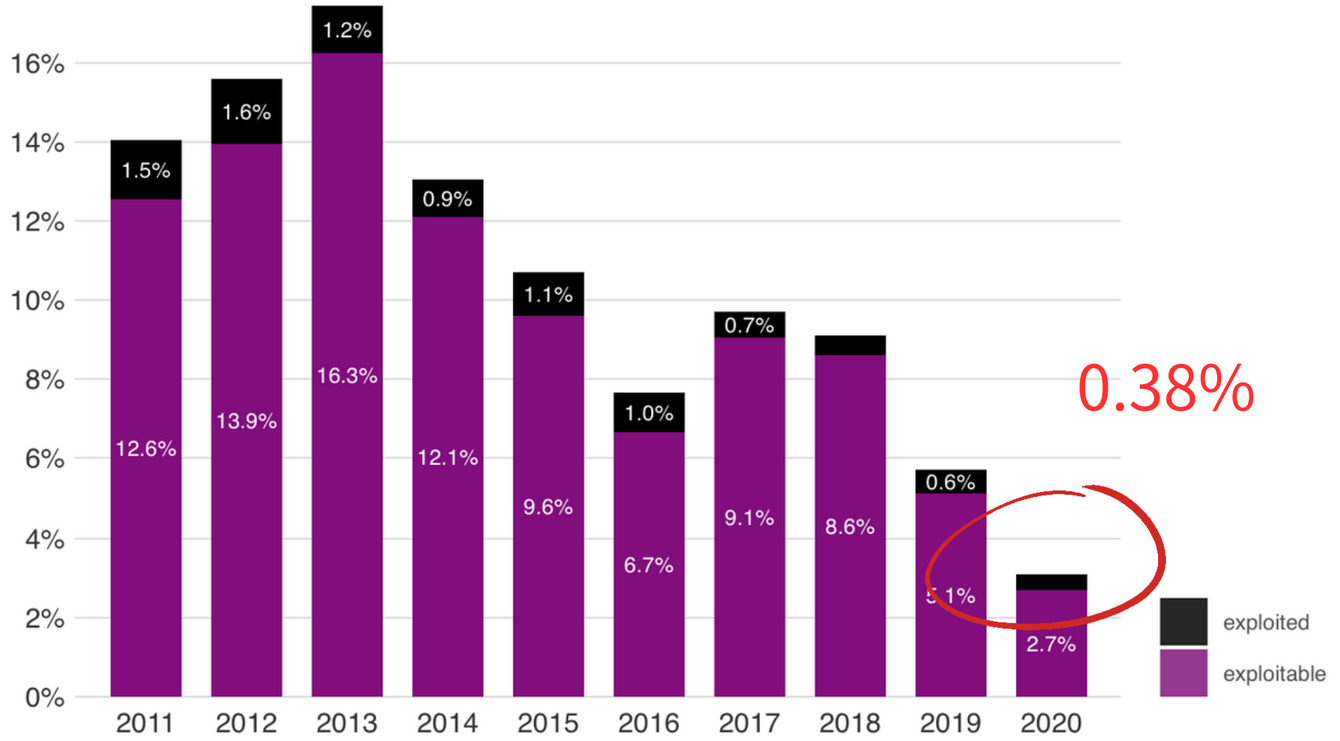
For one vulnerability

- Rezilion: For high-risk vulnerability, it takes longer than 20 Days to patch.

- https://www.rezilion.com/blog/its-about-time-ponemon-report-reveals-how-many-hours-organizations-are-losing-to-vulnerability-management/

Opportunity cost

The percentage of exploited and exploitable Vulnerabilities between 2011 and 2020



Reference: Kenna https://www.kennaresearch.com/a-decade-of-insights/

False positives

CEO of K2 Cyber Security company:

- 75% of Companies Spend as much time on False Positives as on Real Security Events
- 46% of all application downtime is caused by false positives.

https://securityboulevard.com/2021/07/75-of-companies-spend-as-much-time-on-false-positives-as-on-real-security-events/

Business Cases

Business Case 1

Time: 2013
Target: Target Corporation
CVE: CVE-2013-1730
CVSS score: 4.3 (out of 10)

Description:
The attackers gained access to Target's payment system by exploiting a vulnerability in a third-party vendor's software. Which exposed the credit card information of 41 million customers.

USA TODAY:TARGET TO PAY

$28.5M

FOR 2013 DATA BREACH THAT AFFECTED 41 MILLION CONSUMERS

https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/

Business Case 2

Time: 2020
Target: Robinhood
CVE: X
CVSS score: 2.5 (out of 10)

Description:
The attackers gained access to the accounts by exploiting a vulnerability in the company's two-factor authentication (2FA) process. Which resulted in unauthorized access to customer funds. Which affected seven million customers.

CNET:ROBINHOOD TO PAY

$20M

**FOR 2020 DATA BREACH
$19.5 MILLION IN DAMAGES
AND $500,000 IN FEES.**

https://www.cnet.com/personal-finance/banking/robinhood-20-million-settlement-who-is-eligible-for-money/

Agenda

1. Introductions
2. Problem Space
3. **Quick Review**
4. Research & Recommendations
5. Future Work

Current Solution

CVSS

The CVSS model is designed to provide an overall composite score representing the severity and risk of a vulnerability.

- www.first.org

CVSS Scoring System

Base Score

- Reflects Severity
- Largest bearing on the final score
- e.g., Access Vector, Access Complexity, etc.

Temporal Score

- Reflects Urgency
- Exploitability falls into the scope

Environmental Score

- Reflects Priority
- Adjustment that combines Base and Temporal score
- e.g., Collateral Damage Potential, Target Distribution, etc.

3 Quick Review

CVSS is not a THREAT scoring system but an overall evaluation metric for vulnerabilities

Potential Solution

EPSS

The Exploitability Prediction Scoring System calculates the probability a vulnerability will be exploited within the next 30 days.

- www.first.org

3 Quick Review

Produces a probability score between 0 and 1

The higher the score, the greater the probability a vulnerability will be exploited in the next 30 days.

Employs an autoregressive model for threat intelligence

Predicts future exploitability value based on values observed in the past.

Score all vulnerabilities published on MITRE’s CVE List. Update daily.

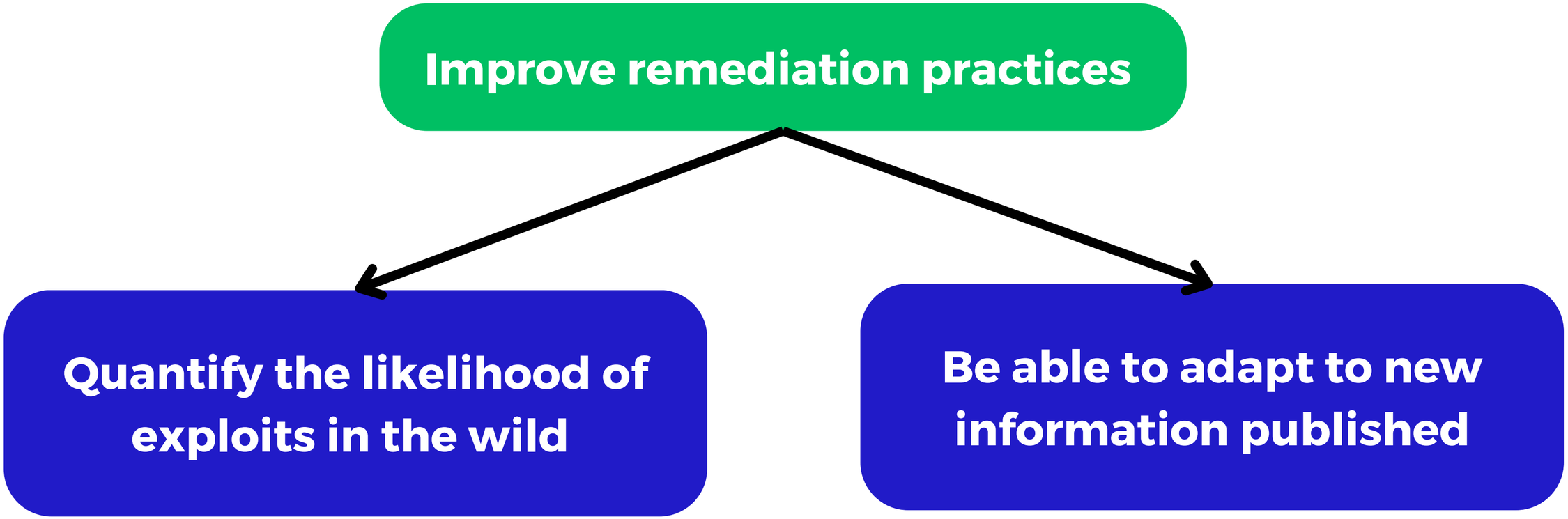
An EPSS reported is released daily for newly scored CVEs. This data can be accessed through a free API with FIRST.

SOURCE: https://www.first.org/epss/model

How was EPSS formed?

- **FIRST's SIG leads EPSS design and creation**
- **Over 170 global members in the SIG**
- **Industry partners share proprietary data for model development.**

The Goal of EPSS



Evolution of EPSS - v1

Features	**lightweight, portable. Implemented in a spreadsheet**
Prediction Model	**Logistic Regression**
Time Frame	**The first whole year**
# of Variables (for training model)	**16**

Evolution of EPSS - v2

Features	**Centralizing and automating data collection and scoring**
Prediction Model	**XGBoost**
Time Frame	**30 Days as of the time of scoring**
# of Variables (for training model)	**1,164**

Evolution of EPSS - v3

EPSS v2

+

- **Improve precision** in identifying exploited vulnerabilities
- **Expand sources** of exploit data
- Introduce methodical **hyper-parameter tuning approach**
- **Improved XGBoost classifier training**
- Achieve **82% improvement** of model over v2

Limit of EPSS

Risk = **Threat** x Vulnerability x Impact

- Measure of threat
- Probability of exploitation activity

- How accessible vulnerable assets are to attackers
- Type of weakness the vulnerability presents
- Severity if exploited

Performance Comparison Between EPSS and CVSS

3 Quick Review

Coverage

The percentage of exploited vulnerabilities that were remediated

Higher when more exploited vulnerabilities are remediated

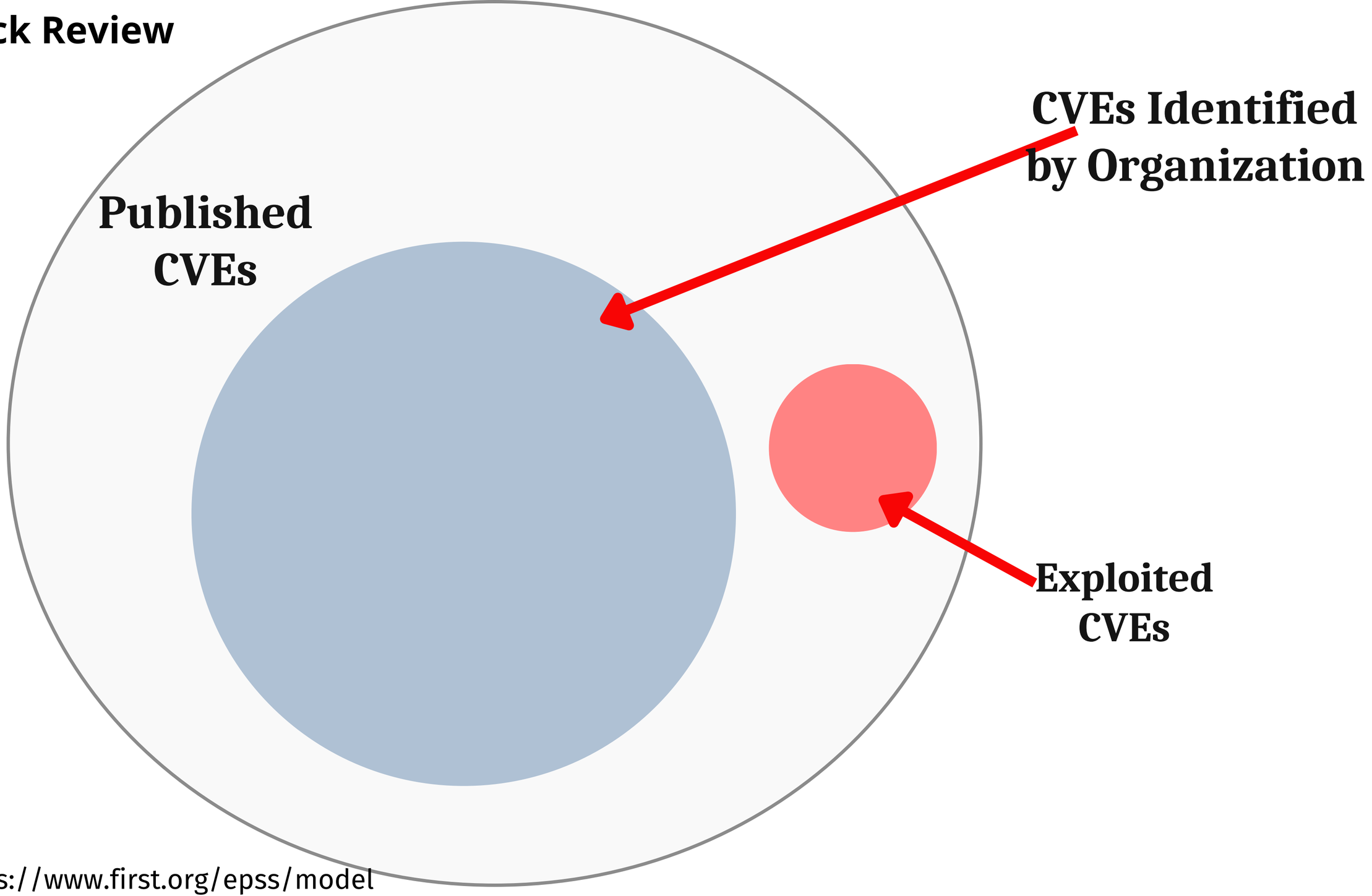
Efficiency

The percentage of remediated vulnerabilities that were exploited

Higher when more exploited vulnerabilities are remediated ***relative to the total number of vulnerabilities patched.***

SOURCE: https://www.first.org/epss/model

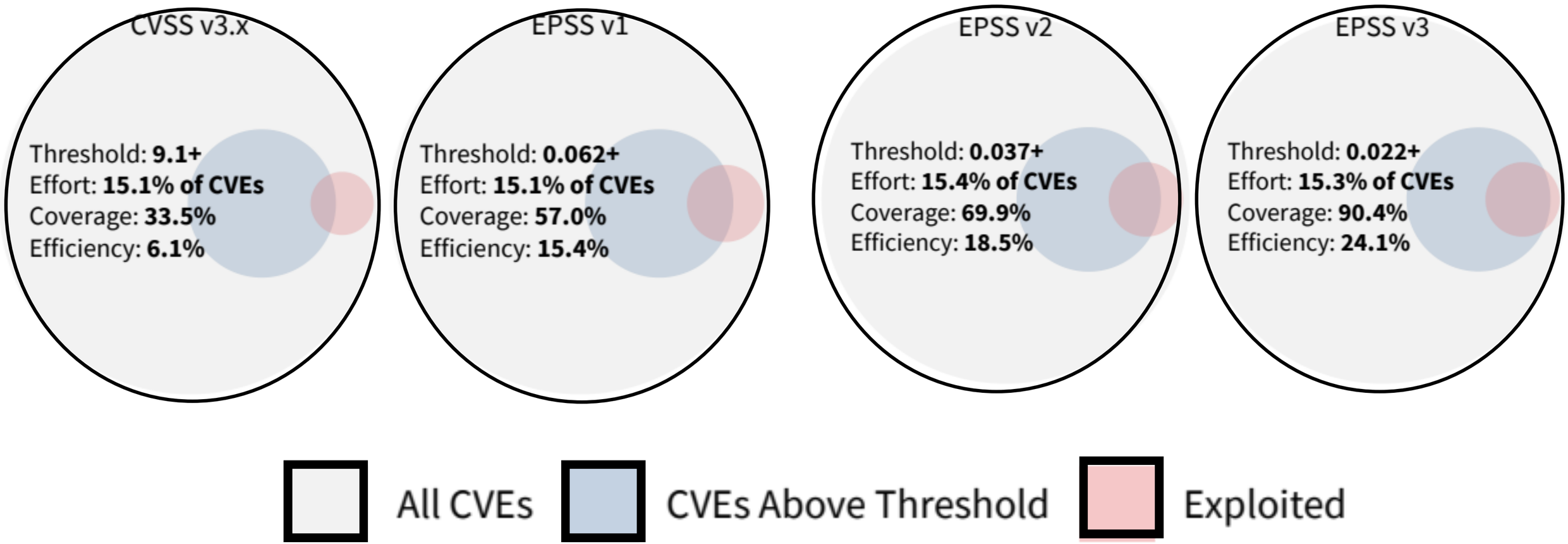
3 Quick Review



SOURCE: https://www.first.org/epss/model

3 Quick Review

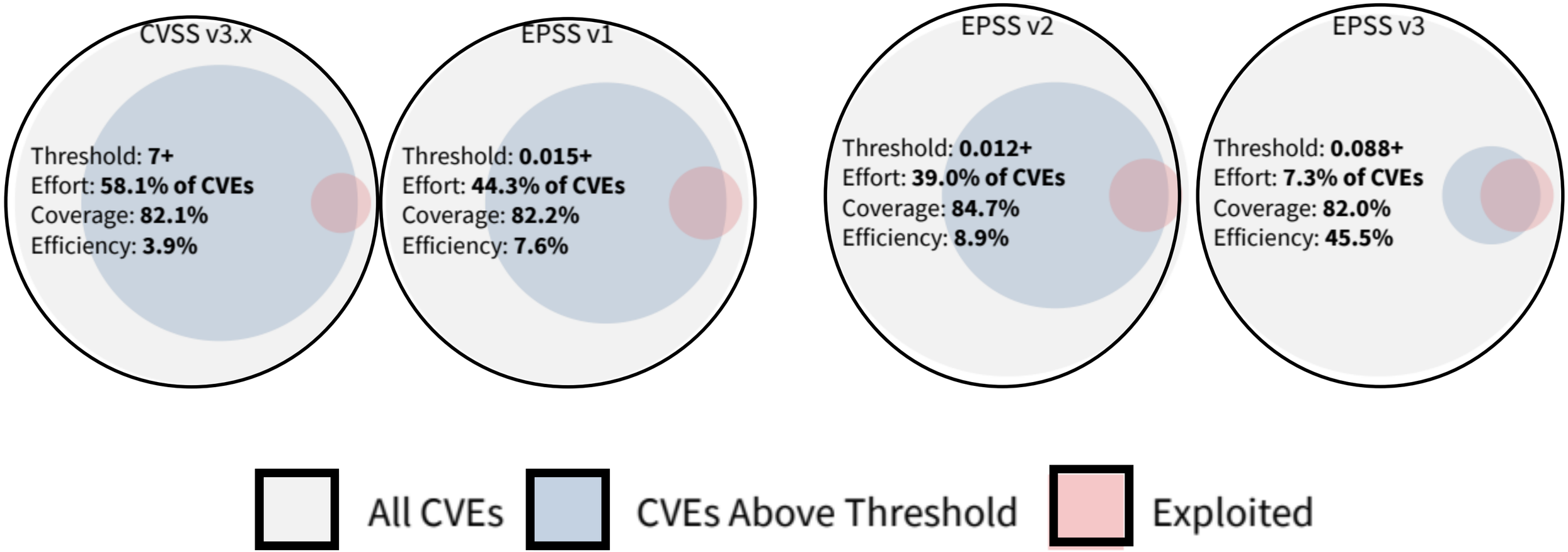
Strategy comparisons holding the level of effort constant



SOURCE: EPSS V3 Reasearch Paper, https://arxiv.org/pdf/2302.14172.pdf

3 Quick Review

Strategy comparisons holding the coverage constant



SOURCE: EPSS V3 Reasearch Paper, https://arxiv.org/pdf/2302.14172.pdf

Results

For almost no increase in effort

~ 3x ↑

Increase in coverage

~ 4x ↑

increase in efficiency

EPSS v3 shows marked increases in efficiency than from CVSS alone.

SOURCE: https://www.first.org/epss/model

Potential Solution

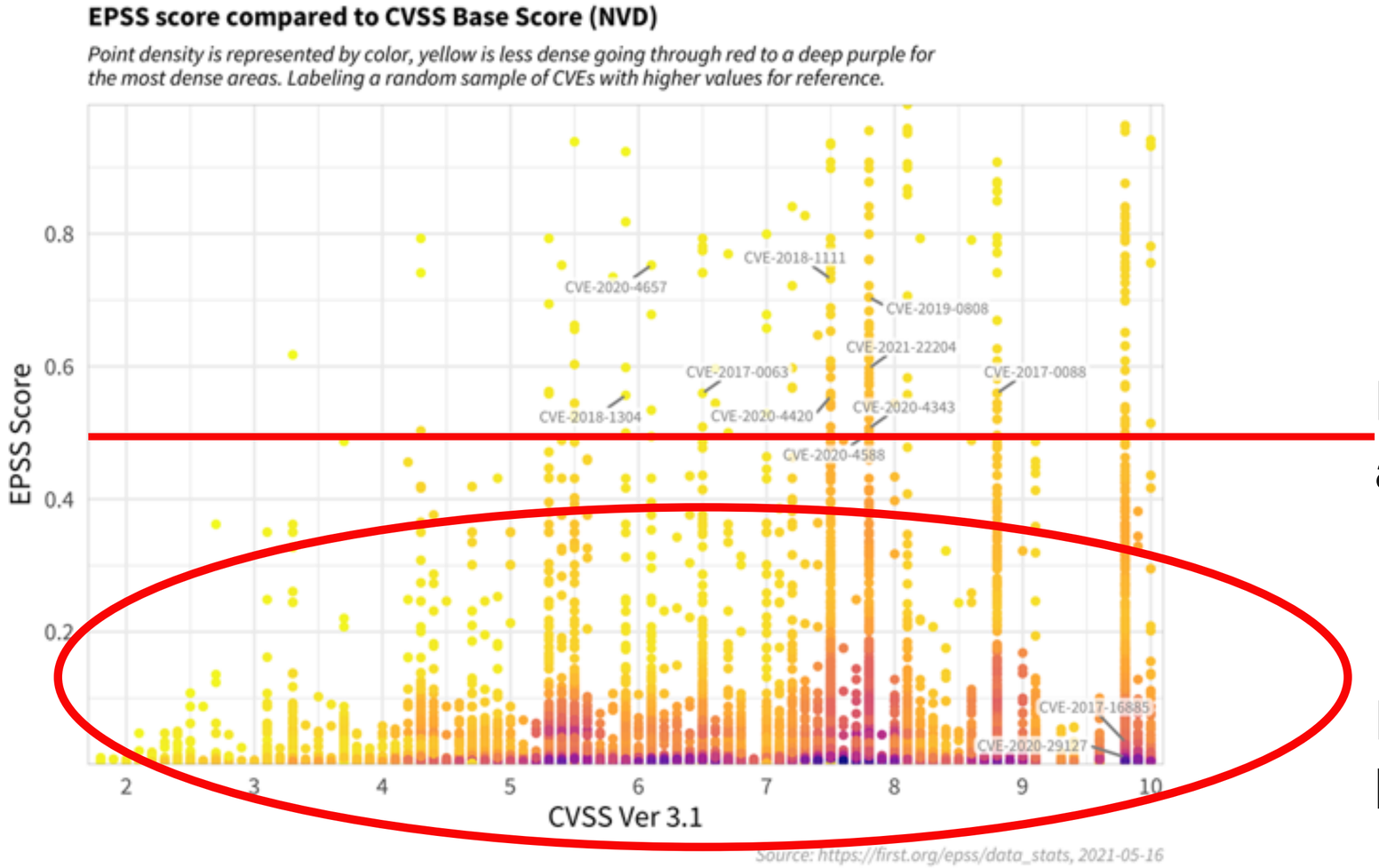
Using EPSS and CVSS Together

EPSS X CVSS?

Multiplying EPSS and CVSS scores is not advisable for the following reasons:

- **Different objectives**
- **Scale incompatibility**
- **Loss of context**
- **Arbitrary interpretation**

3 Quick Review

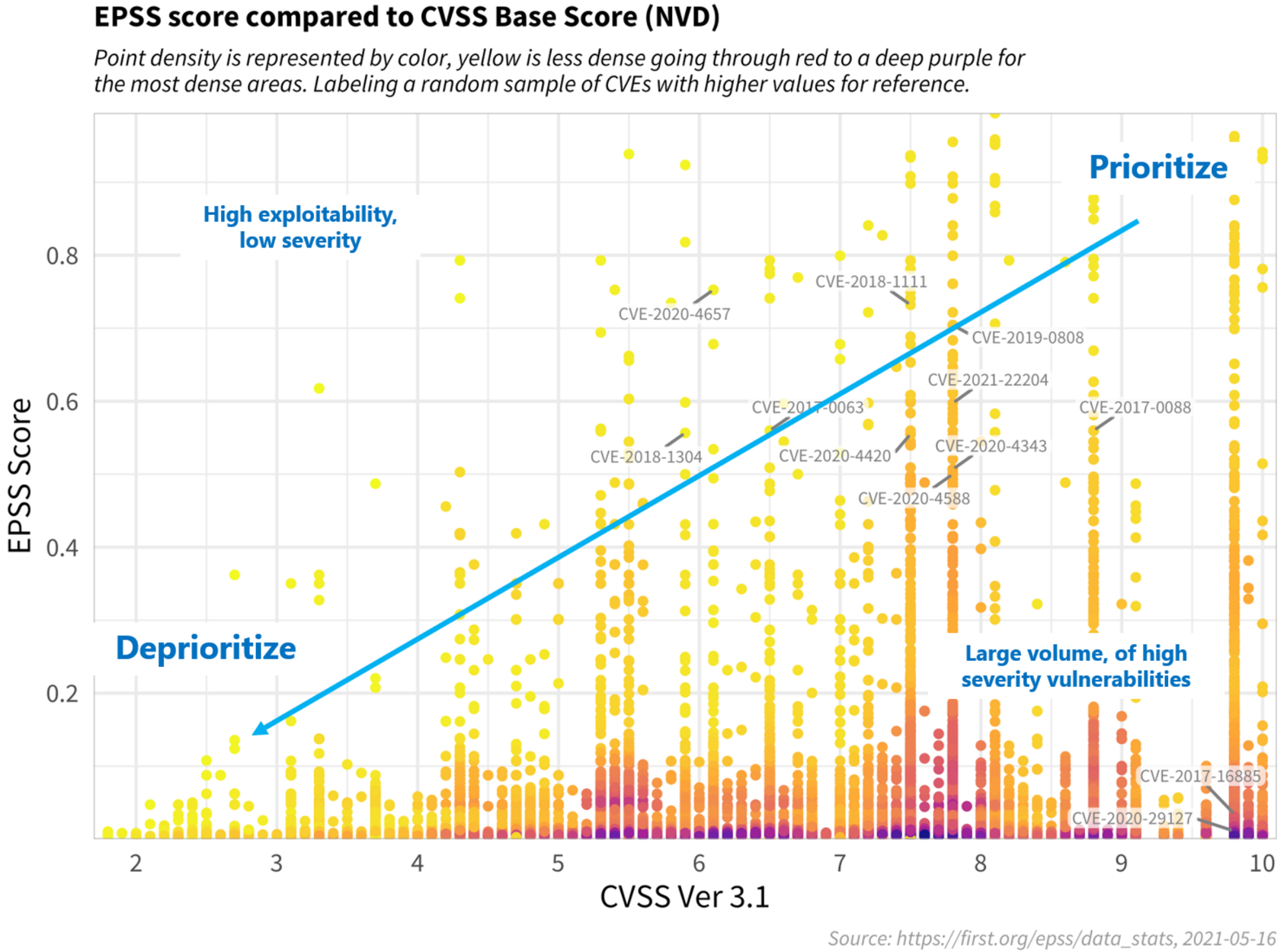


Few vulnerabilities with an EPSS > 0.5

Large concentration on bottom of plot

SOURCE: https://www.first.org/epss/model

3 Quick Review



SOURCE: https://www.first.org/epss/model

Agenda

- Introductions
- Problem Space
- Quick Review
- 4 **Research & Recommendations**
- Future Work

Potential Solution

Unified Vulnerability Scoring System

The integration of different scoring systems into a single, comprehensive approach to vulnerability management.

4 Research and Recommendations

X

Severity (CVSS)

Y

Exploitability (EPSS)

Z

Asset Criticality

Multiply Scores by Assigned Weights and Sum

$$CVSS * \text{Weight } 1$$

$$+$$

$$EPSS * \text{Weight } 2$$

$$+$$

$$Asset\ Score * \text{Weight } 3$$

Example of UVSS Calculation

Example of UVSS Calculation

Vulnerability A

CVSS Score = **8**

EPSS Score = **0.5**

Asset Score = **0.3**

Example of UVSS Calculation

Vulnerability A

CVSS Score = **8**

EPSS Score = **0.5**

Asset Score = **0.3**

Assigned Weights

CVSS Score = **0.3**

EPSS Score = **0.4**

Asset Score = **0.3**

Example of UVSS Calculation

Vulnerability A

CVSS Score = **8**

EPSS Score = **0.5**

Asset Score = **0.3**

Assigned Weights

CVSS Score = **0.3**

EPSS Score = **0.4**

Asset Score = **0.3**

Risk Score = CVSS*Weight + EPSS*Weight + Asset* Weight

Example of UVSS Calculation

Vulnerability A

CVSS Score = **8**

EPSS Score = **0.5**

Asset Score = **0.3**

Assigned Weights

CVSS Score = **0.3**

EPSS Score = **0.4**

Asset Score = **0.3**

Risk Score = CVSS*Weight + EPSS*Weight + Asset* Weight

Risk Score = (8*0.3) + (0.5*0.4) + (0.3*0.3)

Example of UVSS Calculation

Vulnerability A

CVSS Score = **8**

EPSS Score = **0.5**

Asset Score = **0.3**

Assigned Weights

CVSS Score = **0.3**

EPSS Score = **0.4**

Asset Score = **0.3**

Risk Score = CVSS*Weight + EPSS*Weight + Asset* Weight

Risk Score = (8*0.3) + (0.5*0.4) + (0.3*0.3)

Risk Score = 2.69

Normalize CVSS Scores to Balance Weights

$$\frac{\text{CVSS}}{\text{Max CVSS Value}}$$

The maximum CVSS value a vulnerability can have is 10

Example of UVSS Calculation Post-Normalization

Vulnerability A

Normalized CVSS Score = **0.8**

EPSS Score = **0.5**

Asset Score = **0.3**

Assigned Weights

CVSS Score = **0.3**

EPSS Score = **0.4**

Asset Score = **0.3**

Risk Score = CVSS*Weight + EPSS*Weight + Asset* Weight

Risk Score = (**0.8***0.3) + (0.5*0.4) + (0.3*0.3)

Risk Score = 0.53

Benefits of UVSS

More comprehensive and accurate risk assessment

Improved resource allocation

Customizable to the needs of Capital One

4 Research and Recommendations

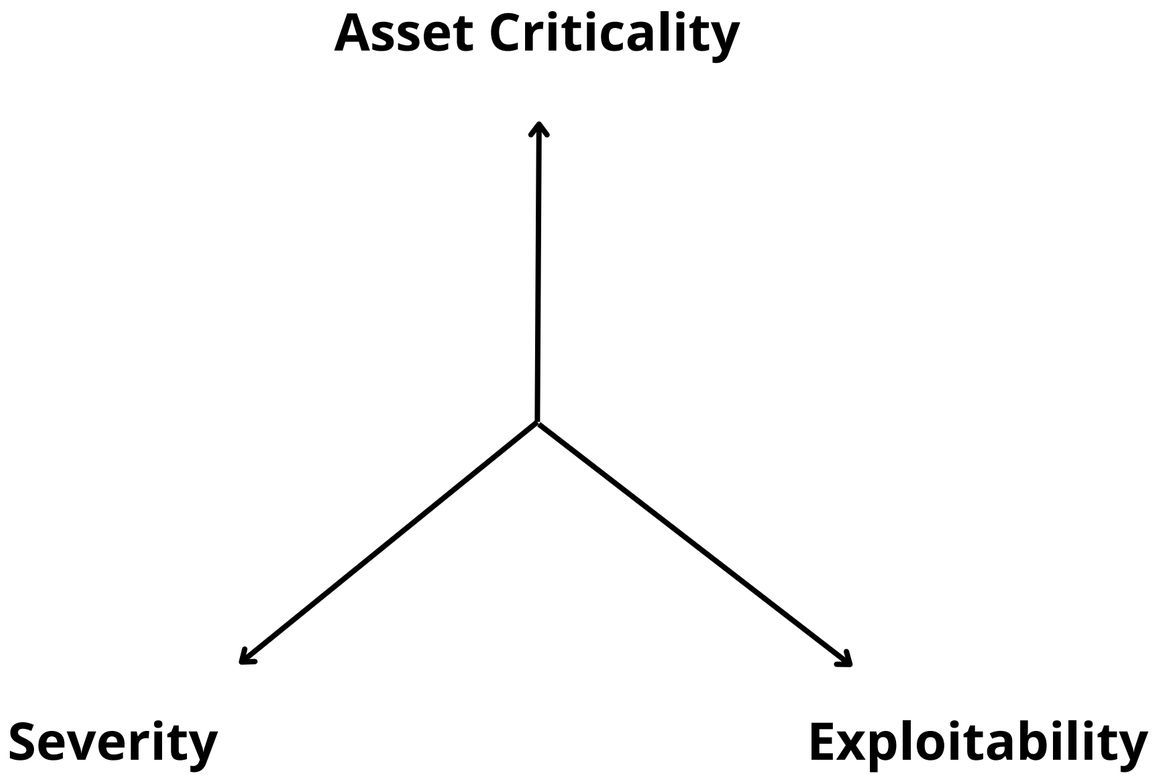
DEMO

https://cmu-exploitability-capstone-2023.shinyapps.io/rshiny/

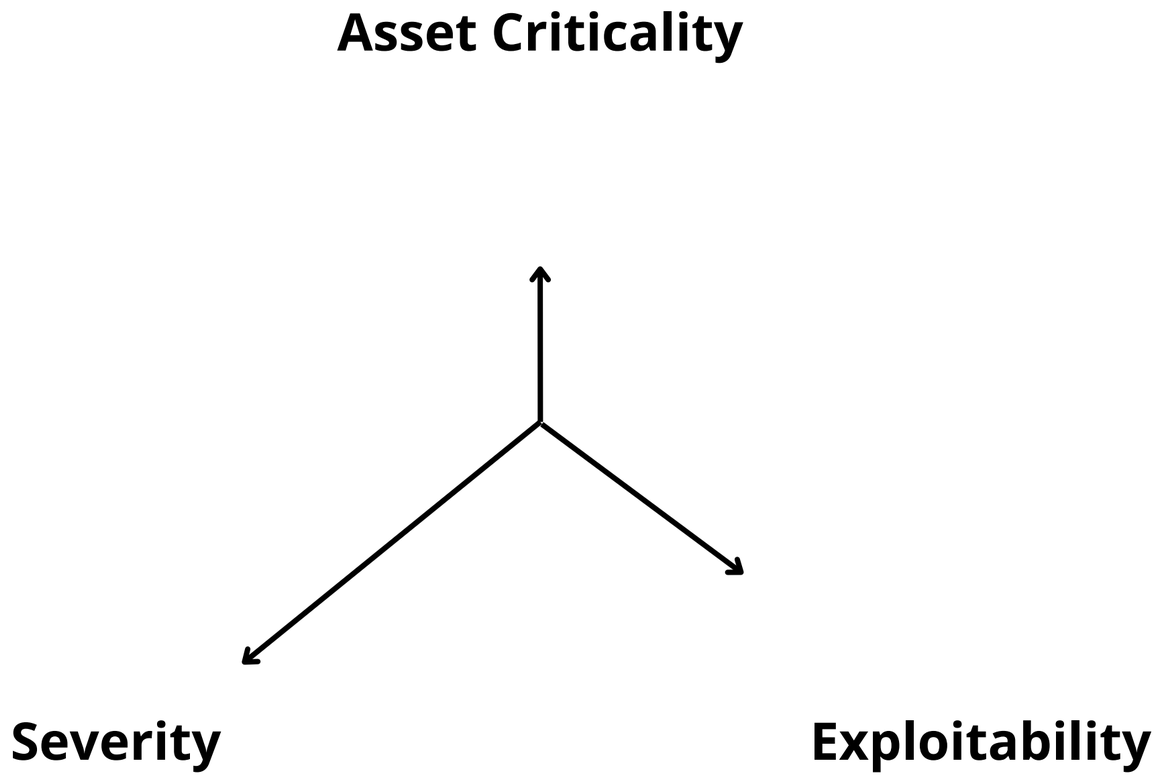
Potential Solution

Point Capture Approach

4 Research and Recommendations

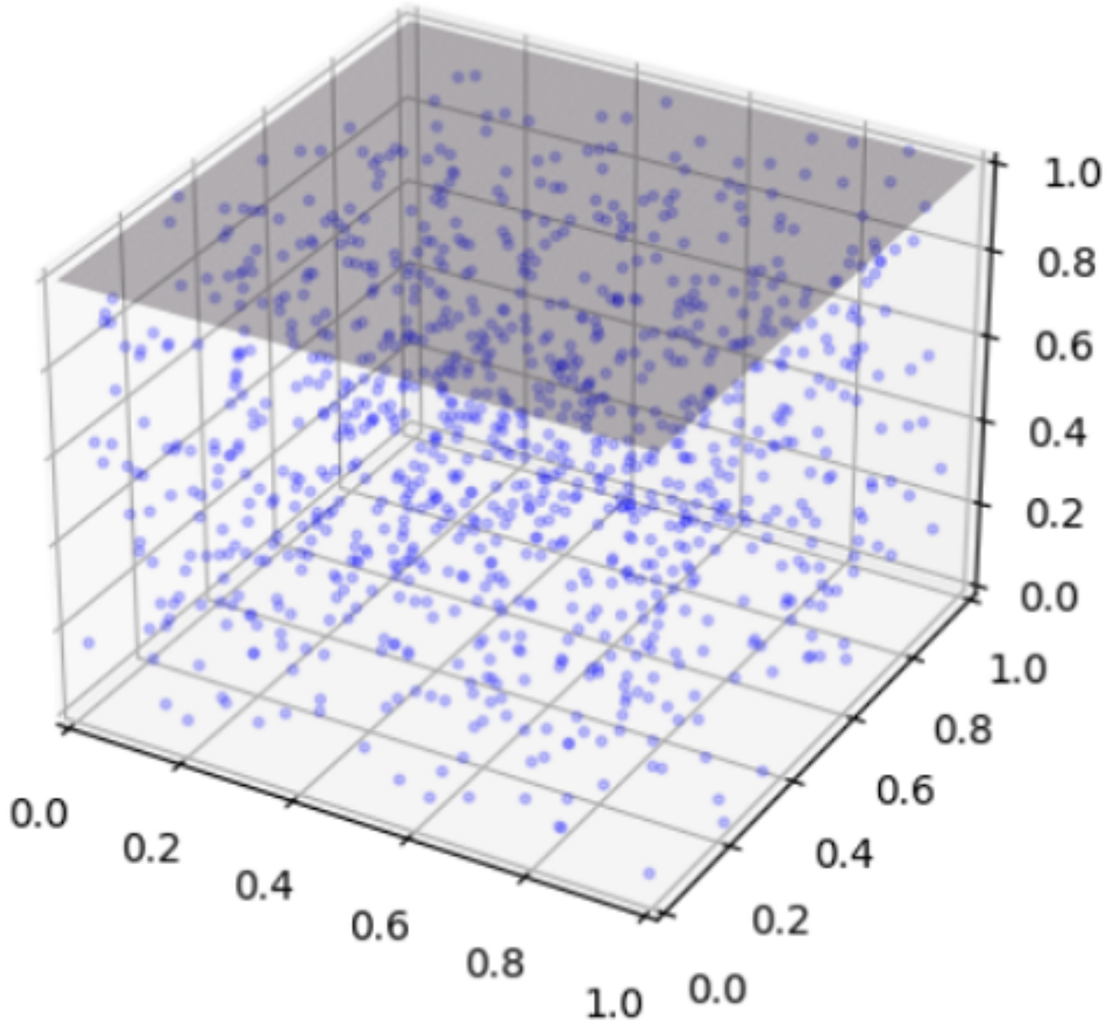


4 Research and Recommendations



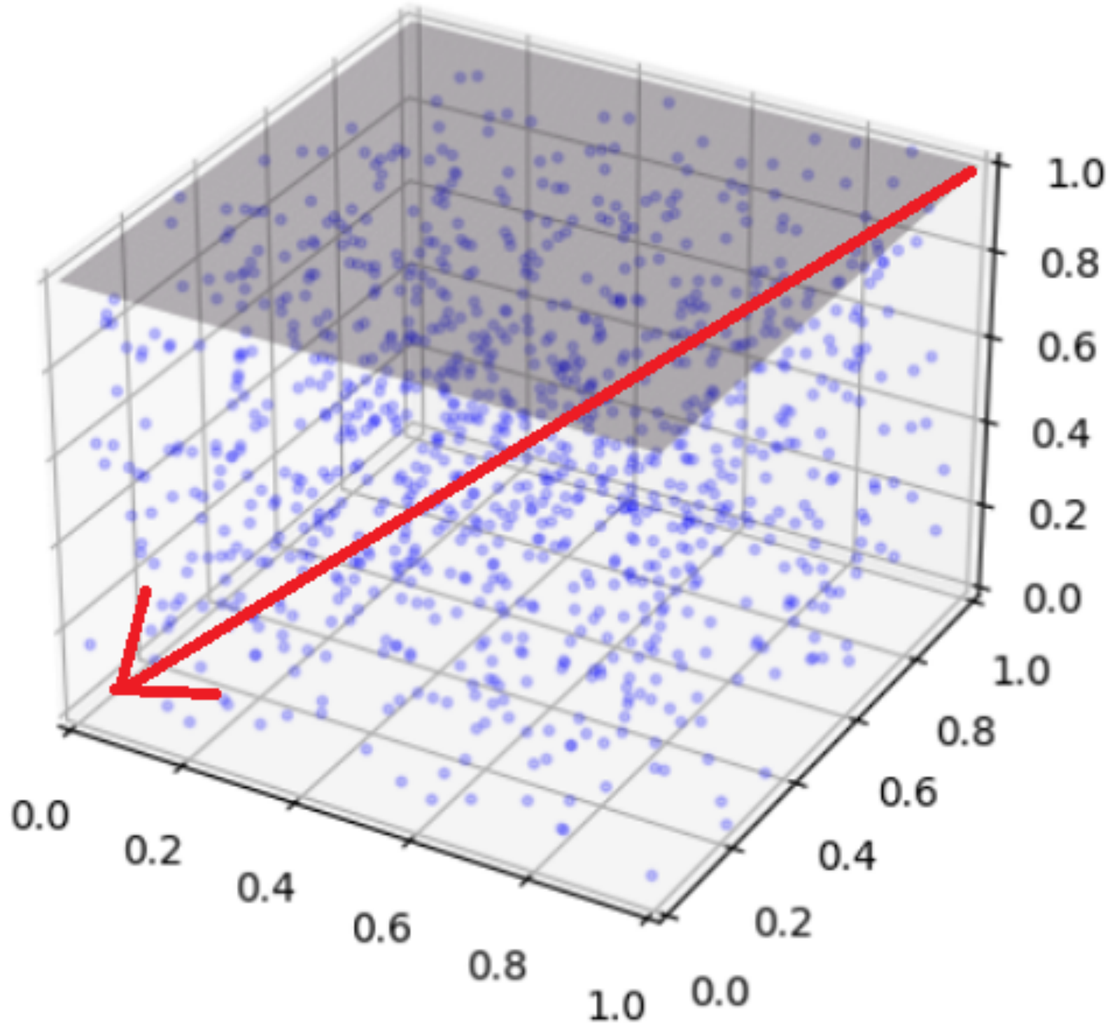
4 Research and Recommendations

Point Capture Approach - Explain



4 Research and Recommendations

Point Capture Approach - Explain

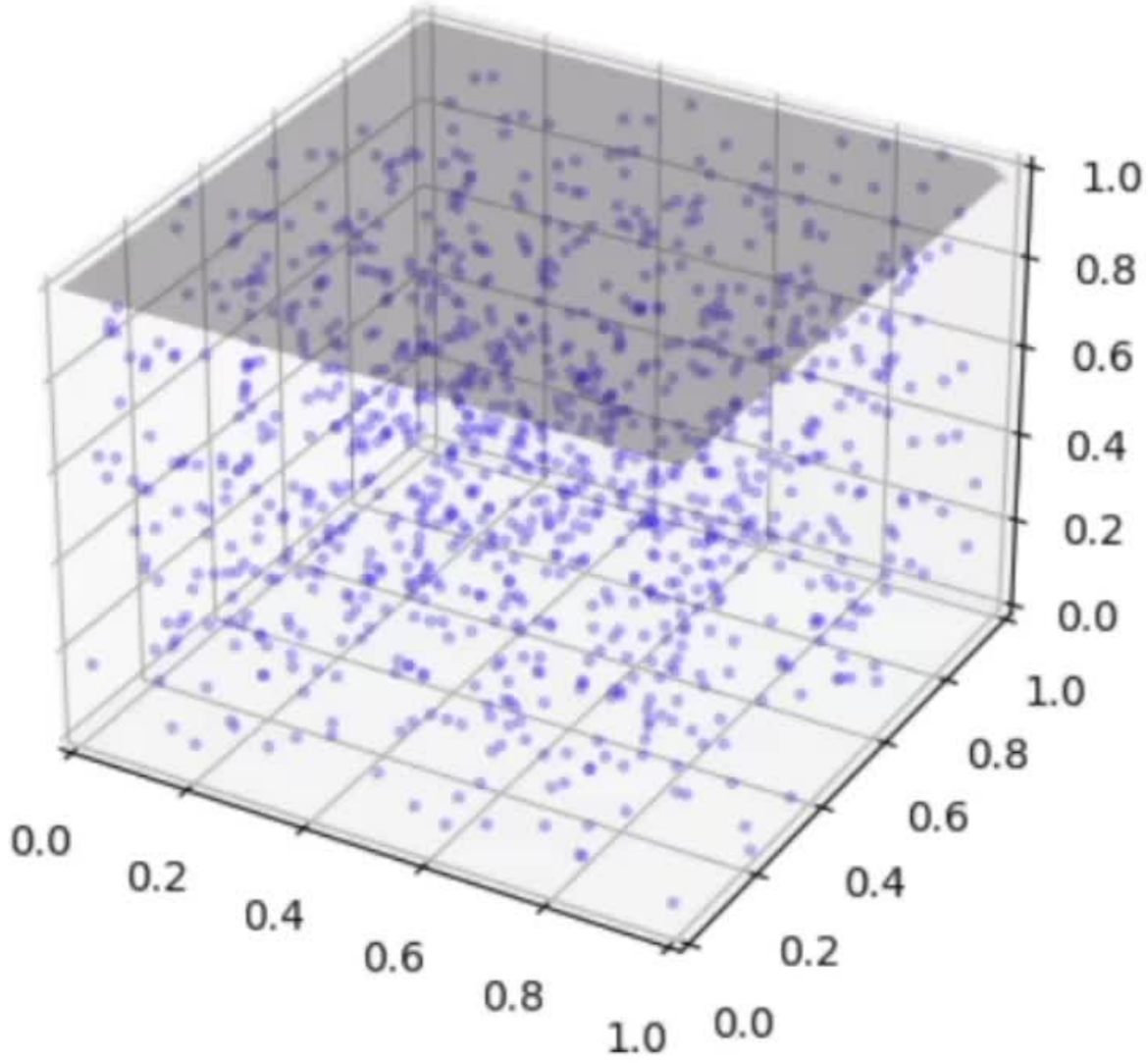


Point Capture Approach - Explain

$$Sum = x + y + z$$

4 Research and Recommendations

Point Capture Approach - Explain

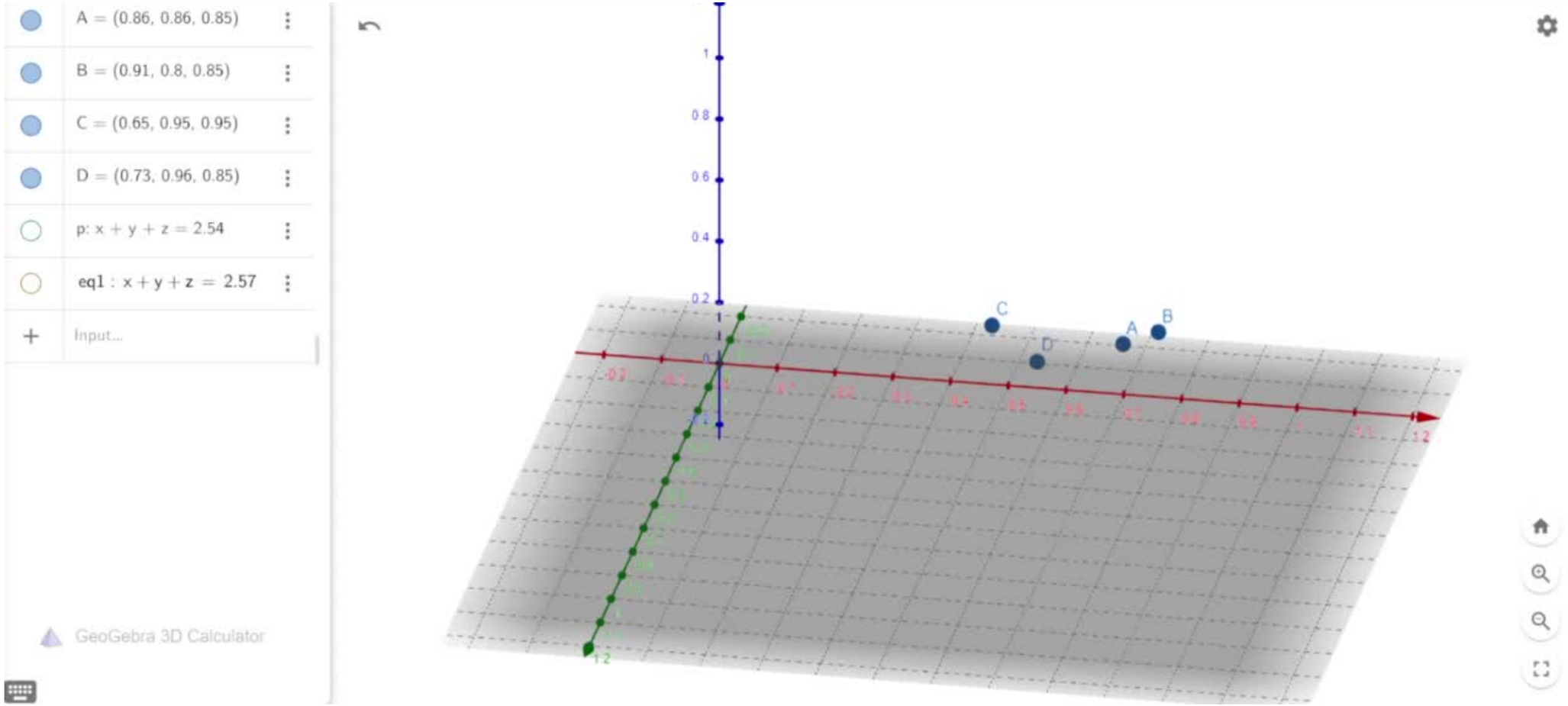


Point Capture Approach - Explain

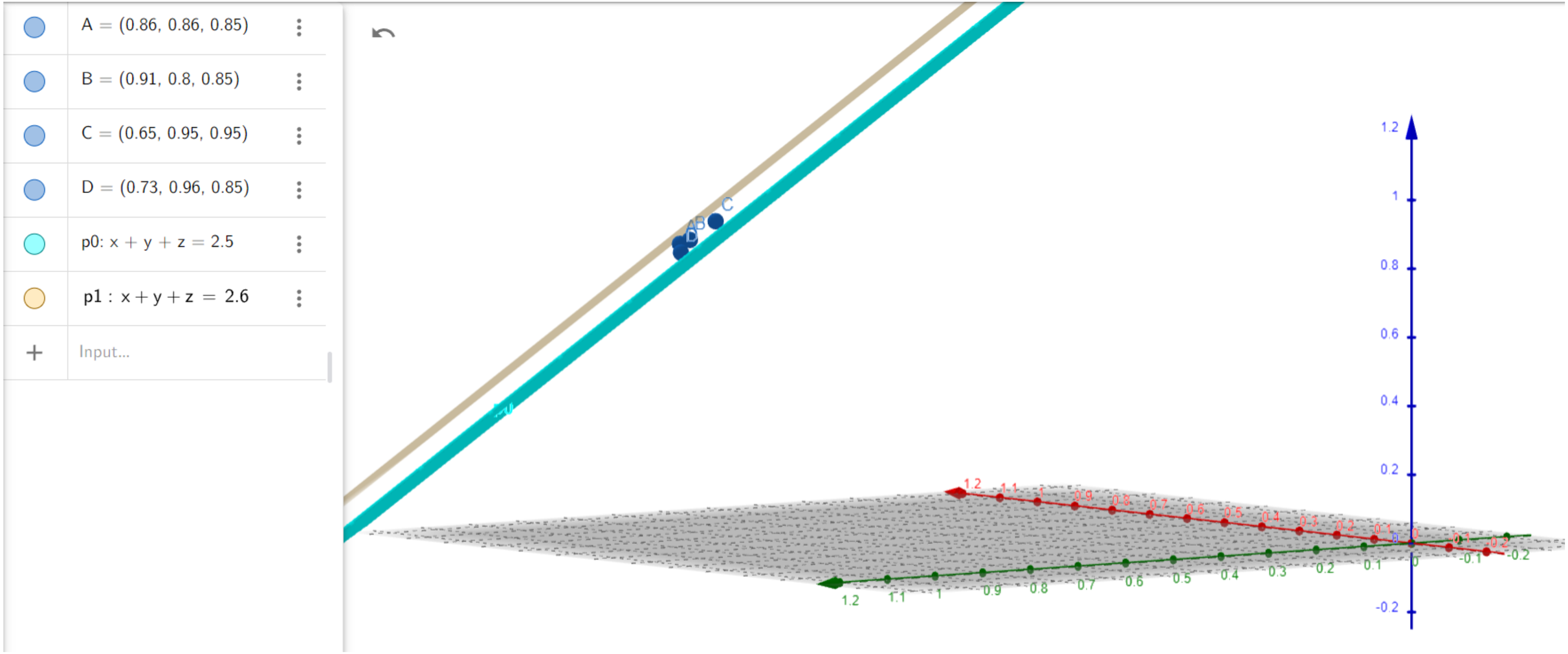
Sum = x + y + z

x	y	z	sum
0.86	0.862	0.85	2.57
0.88	0.72	0.97	2.57
0.91	0.8	0.85	2.56
0.65	0.95	0.95	2.55
0.73	0.96	0.85	2.54

Point Capture Approach - Explain



Point Capture Approach - Explain



Point Capture Approach - Summary

- Have equal weight on a global scale.
- Select an interval that would group points together.
- Starting From (1,1,1) to (0,0,0)
- Find the most significant point
- Apply the interval.
- For the points inside two plane
  - Sort with weight. (Local weighed)
- Repeated for the next group

Agenda

1. Introductions
2. Problem Space
3. Quick Review
4. Research & Recommendations
5. **Future Work**

Future Work

UVSS does not consider how accessible a vulnerability is to threat actors.

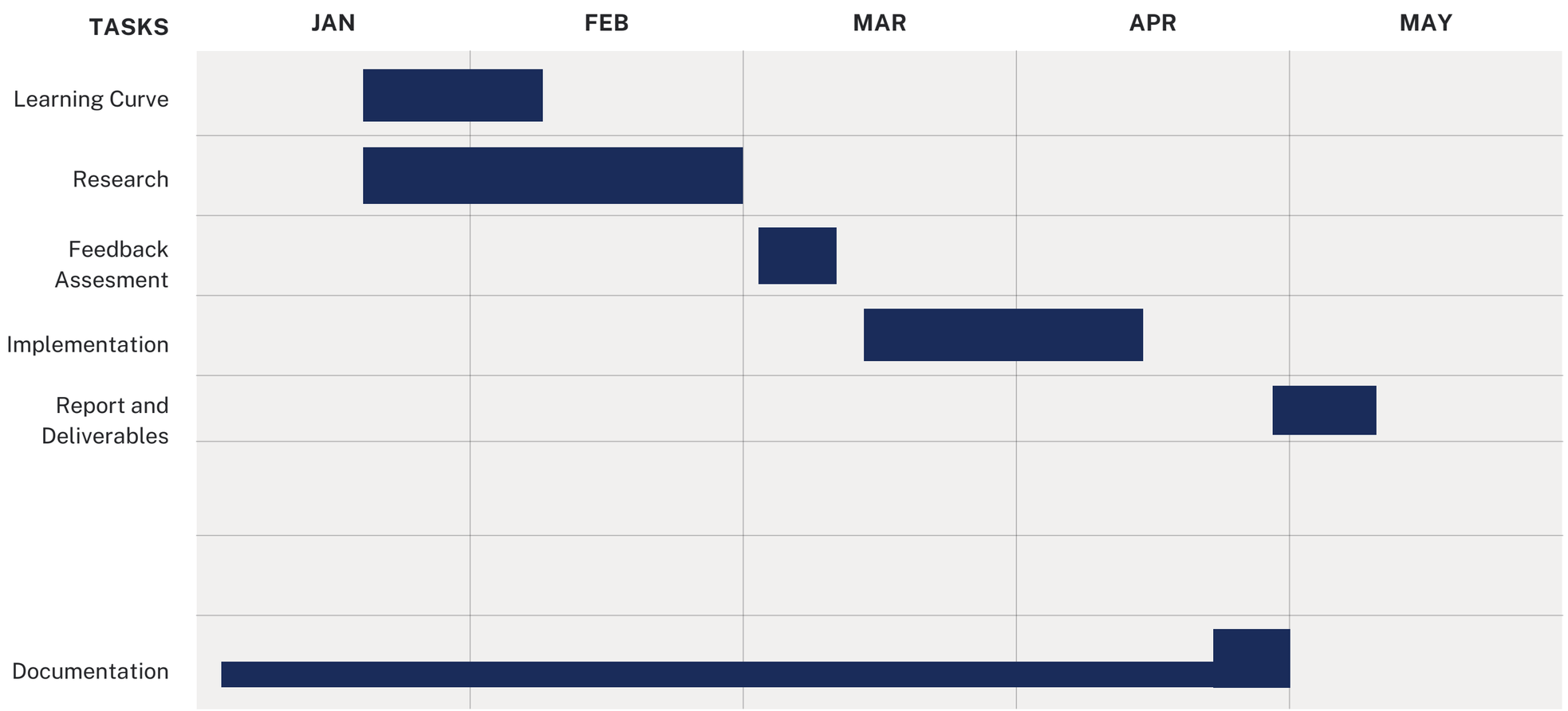
Extending the multi-dimensionality aspect.

Determining weights on a use-case basis.

Performance analysis on the model.

PROGRESS TRACKER

Come up with workable, data-backed v1 Scoring System



Thank you

Q&A