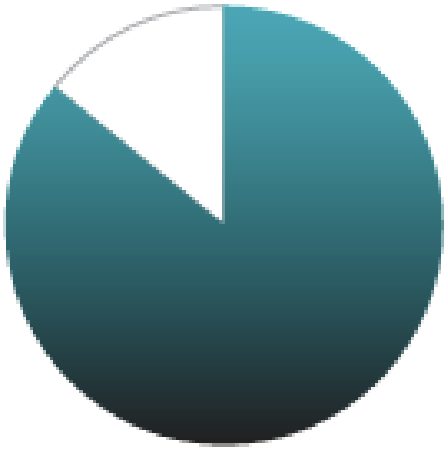
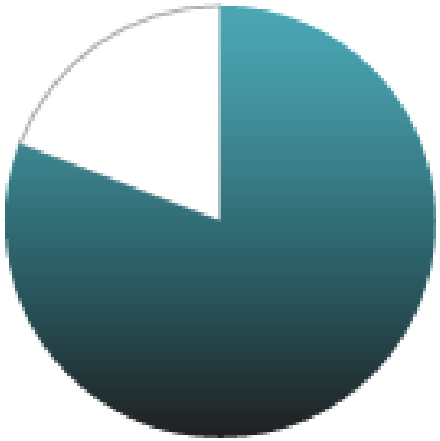
How Does Security Practice Adoption Impact Security Outcome Metrics Over Time?

Jill Marley
Advisor: Dr. Laurie Williams

Vulnerable Dependencies



86% of codebases contained vulnerable open source dependencies



81% of codebases contained high- or critical-risk vulnerabilities

Black Duck *2025 Open Source Security and Risk Analysis report*

Software Security Frameworks

SLSA

NIST National Institute of Standards and Technology U.S. Department of Commerce

Secure Software Development Framework (SSDF)

Secure Supply Chain Consumption Framework (S2C2F)

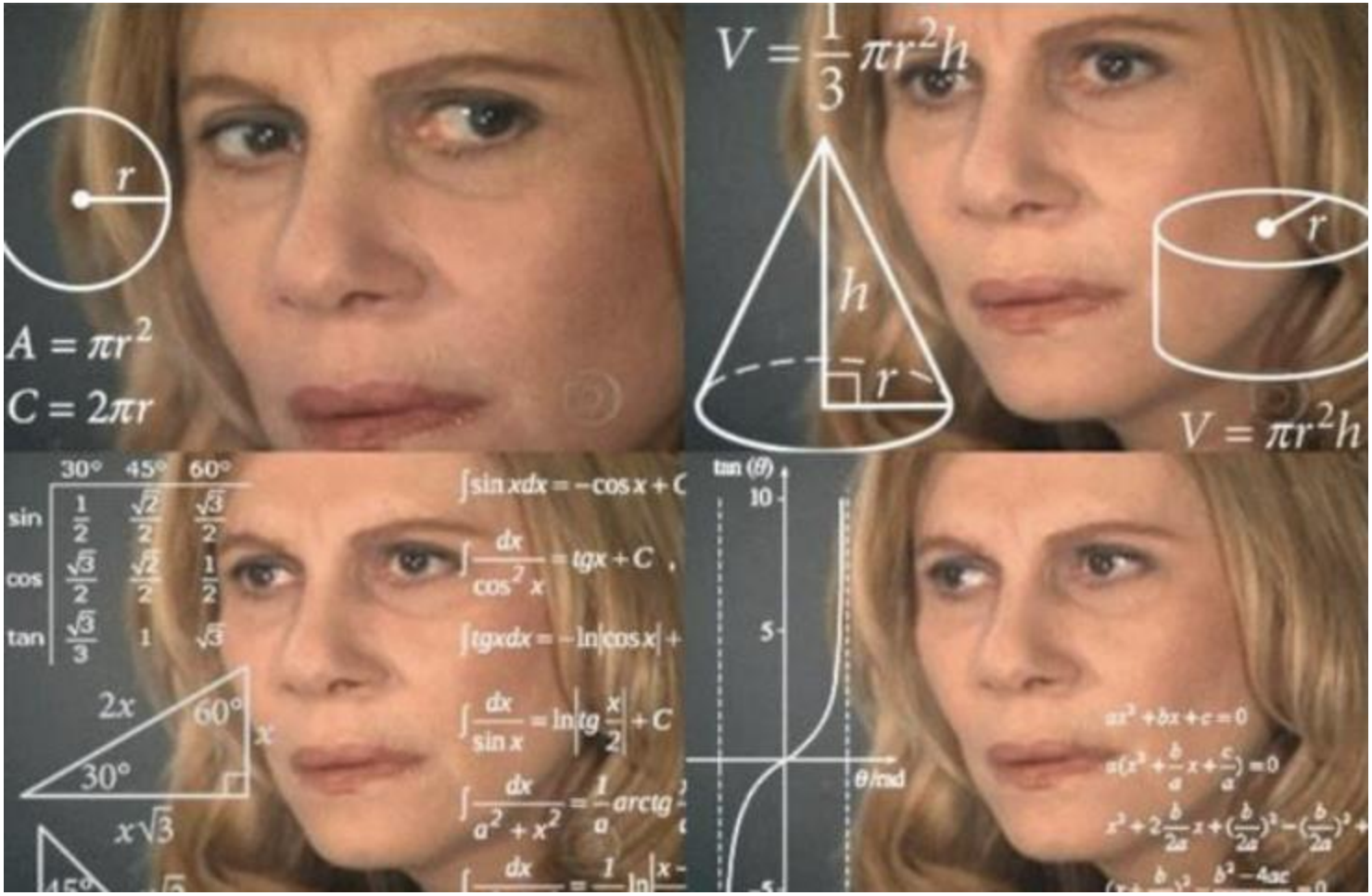
Microsoft continues improving the Framework in partnership and collaboration with the OpenSSF.

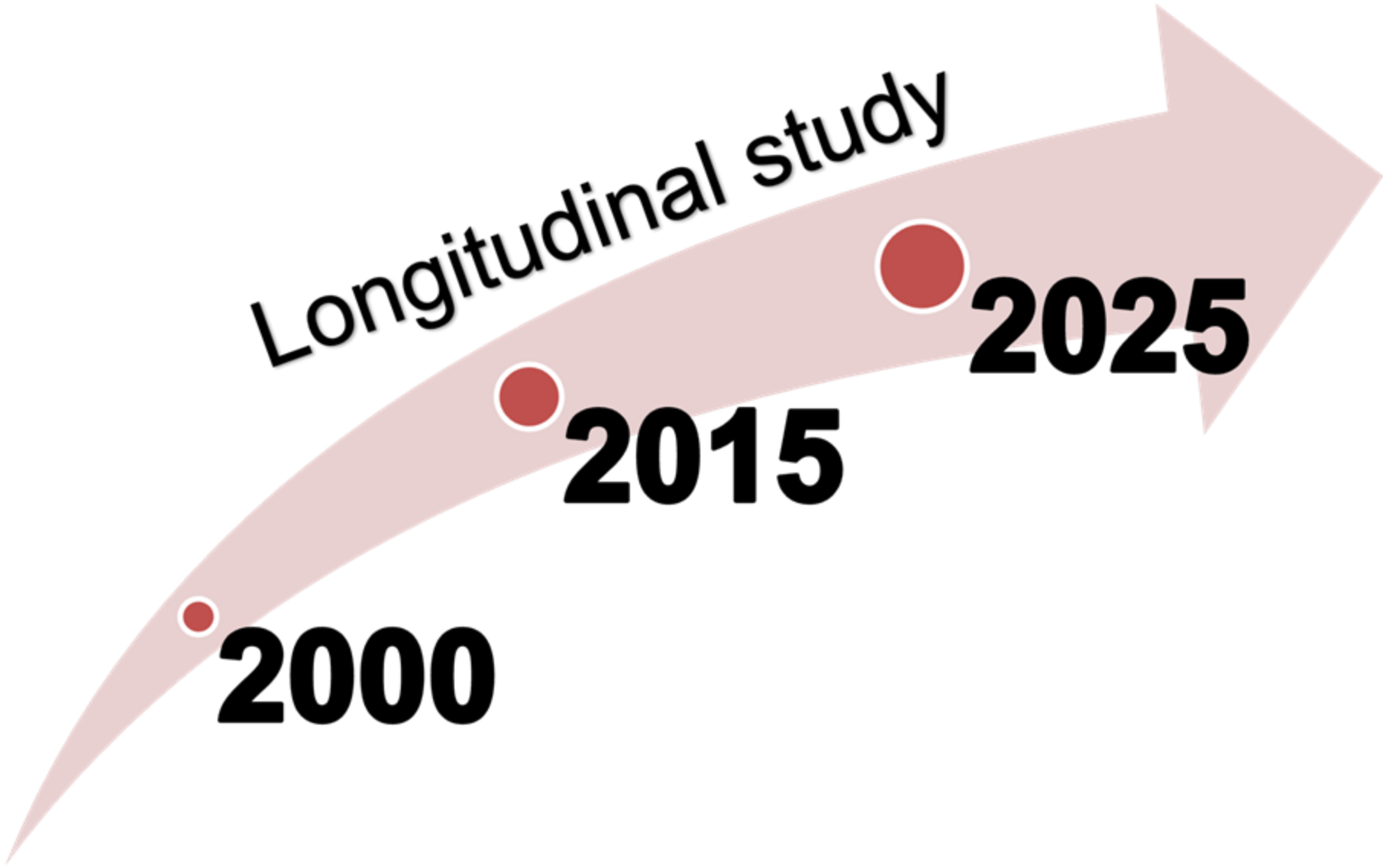
OpenSSF
OPEN SOURCE SECURITY FOUNDATION

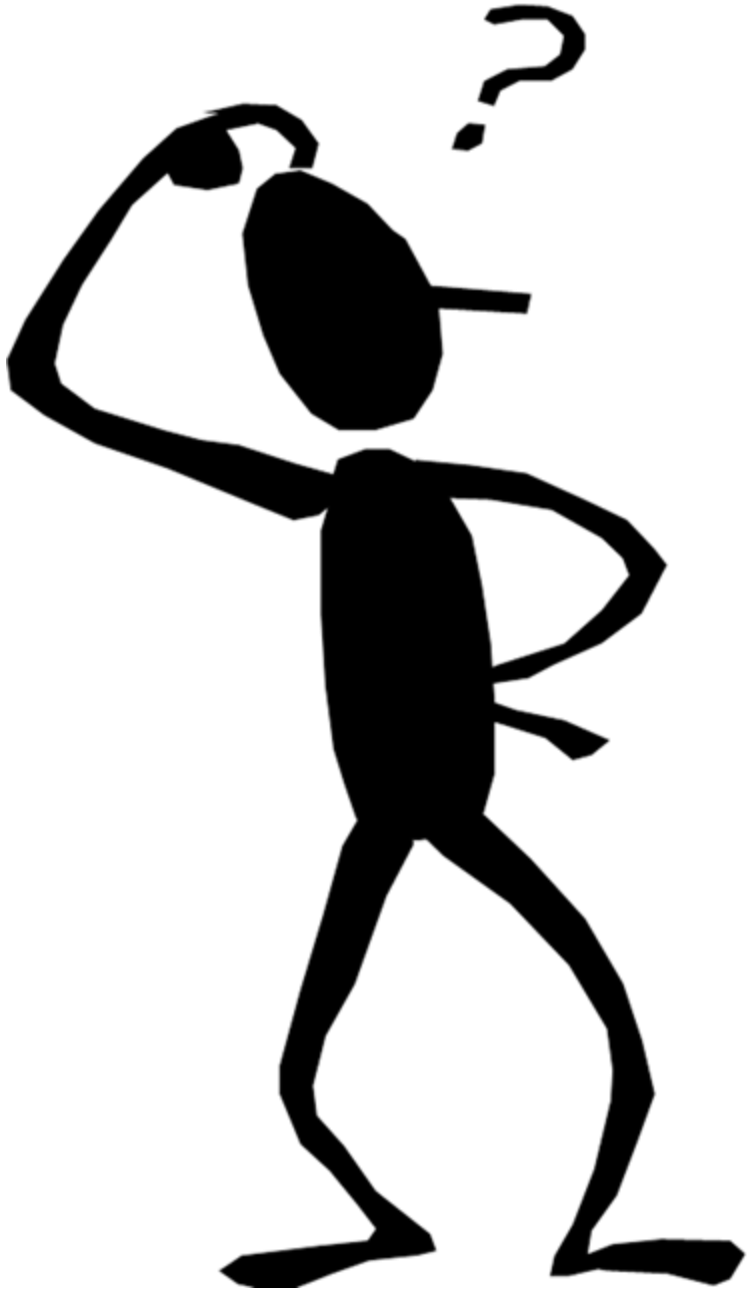
Scorecard

Proactive Software Supply Chain Risk Management Framework

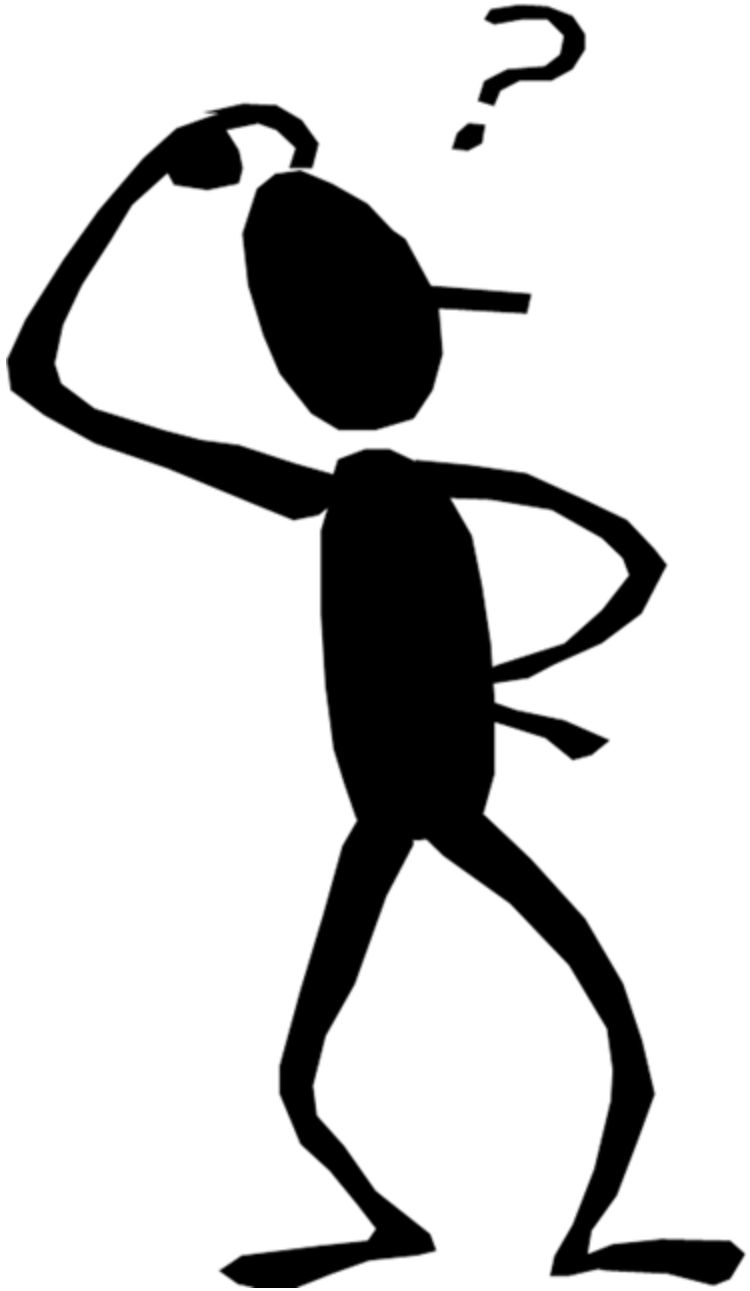
More security practices, more vulnerabilities?




Longitudinal study
2000
2015
2025

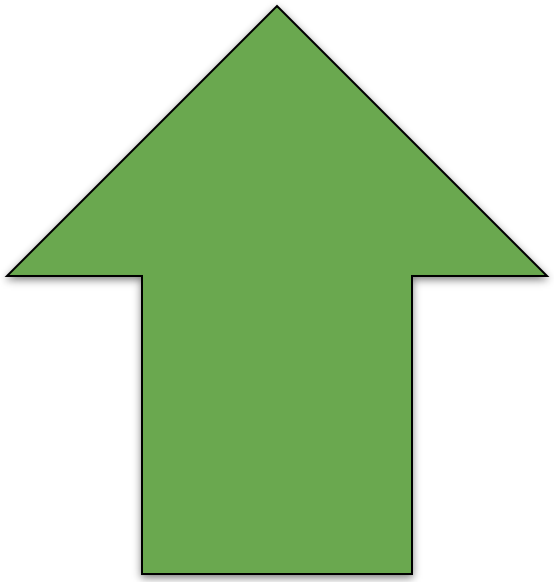


When software practitioners adopt security practices, do their security outcome metrics improve over time?



More specifically, we want to investigate if adopting security practices *causes* security outcome metrics to improve through causal analysis.

Hypothesis



Increase in Practice Adoption

leads to

Better Security Outcomes

Goal: Empirical Evidence

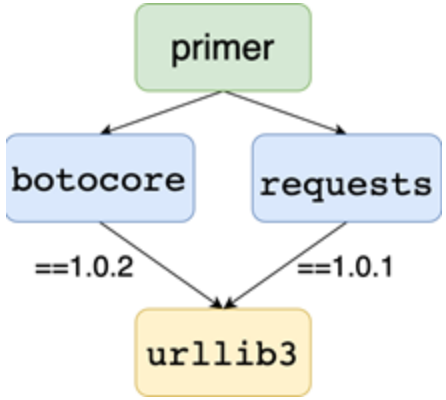
Measuring Practice Adoption: OpenSSF Scorecard

Measuring Practice Adoption: OpenSSF Scorecard

Examples of Scorecard Metrics

Code Review

Contributors



Pinned Dependencies

Security Outcome Metrics

1. Vulnerability Count

The number of publicly disclosed or reported vulnerabilities within a project

Security Outcome Metrics

2. Mean Time To Update (MTTU)

The average aggregated time a package uses outdated direct dependencies in its lifetime

Security Outcome Metrics

3. Mean Time To Remediate (MTTR)

The average aggregated time a package uses outdated and vulnerable direct dependencies in its lifetime.

Dataset: Inclusion and Exclusion Criteria

Including ✅:

+

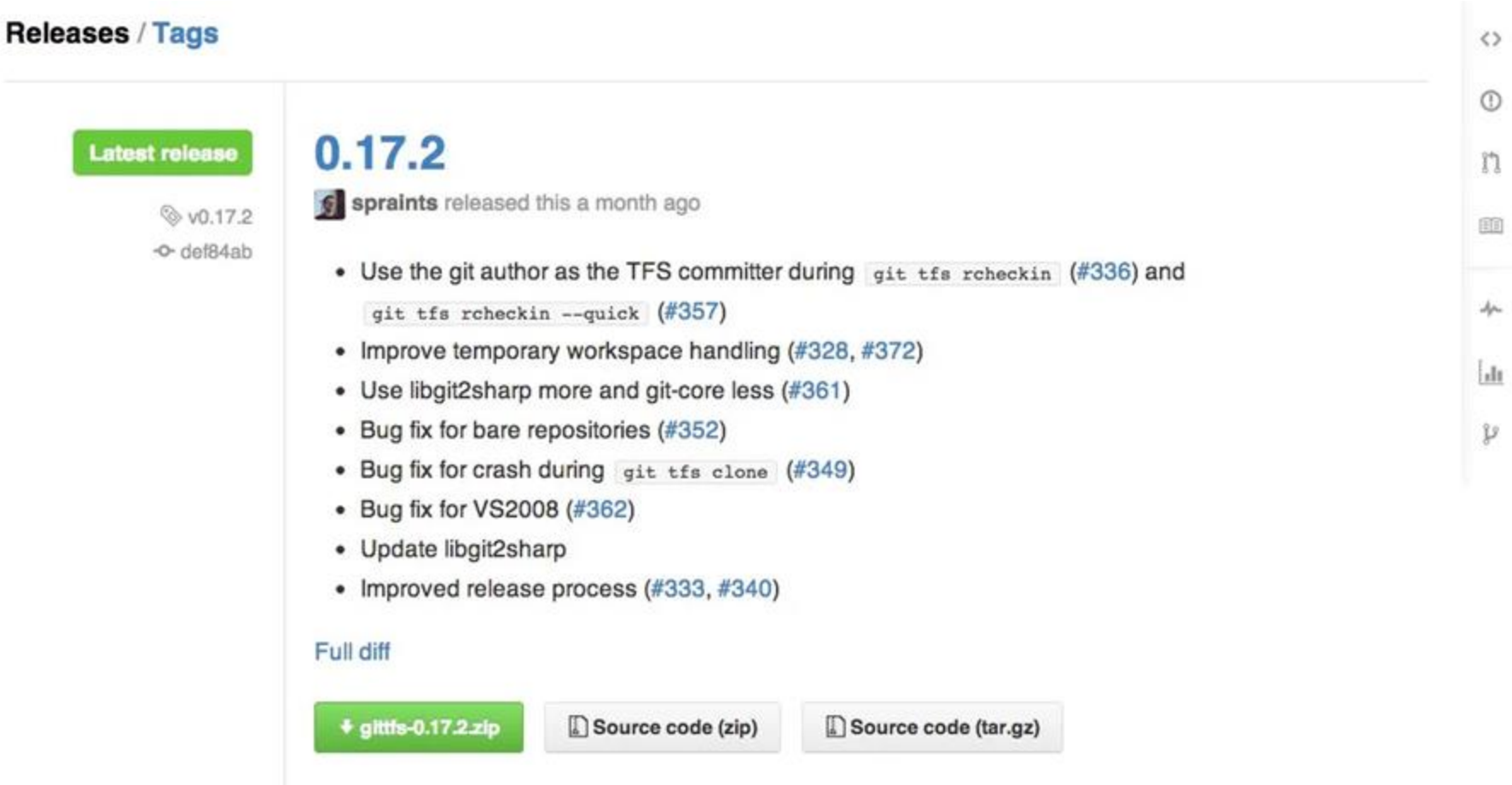
with

- Packages with at least one dependent and dependency
- At least 2 years old

Excluding ❌:

- Repositories that contain multiple packages

GitHub Release



Dataset Overview

- ~14k packages
- October 2023 - October 2025
- For each package release:
  - Scorecard metrics
  - Security outcome metrics
  - Control variables

What are the trends we can identify in Scorecard score changes?

How do changes in individual Scorecard metrics over time affect vulnerability count, MTTU, and MTTR?

Given practice adoption, how long does it take for the security outcome metric to improve, after controlling for (our control variables)?

Thank you!

Any thoughts? Contact me:

Jill Marley
jahmad5@ncsu.edu