Detecting Unsafe Updates in Software Ecosystems

Yao-Wen Chang

September 27, 2023

Supervised by: Christoph Treude
Co-supervised by: Behnaz Hassanshahi (Oracle Labs, Australia)

BACKGROUND

- **SolarWind's Orion** platform is polluted.
- Malicious action against **Esline-Scope**.

OBJECTIVE

- Introduce a new framework.
- Evaluate the effectiveness of the framework.
- Automate the unsafe update explore process.

Research Questions

1. *What is the scope of the impact of the risks that exist within our target Python and Java repositories?*
2. *What are the results if these suspicious updates from contributors in open source projects compromise the target?*
3. *To what extent does this work enhance the security of CI/CD pipelines based on the findings and recommendations from our research?*

OUTLINE

- Related Works
- Research Methods
  - Data Source
  - Framework
  - Pipeline
  - Metric
- Summary
- QA

RELATED WORKS

Regex

Introduce papers....

Machine Learning

Introduce papers....

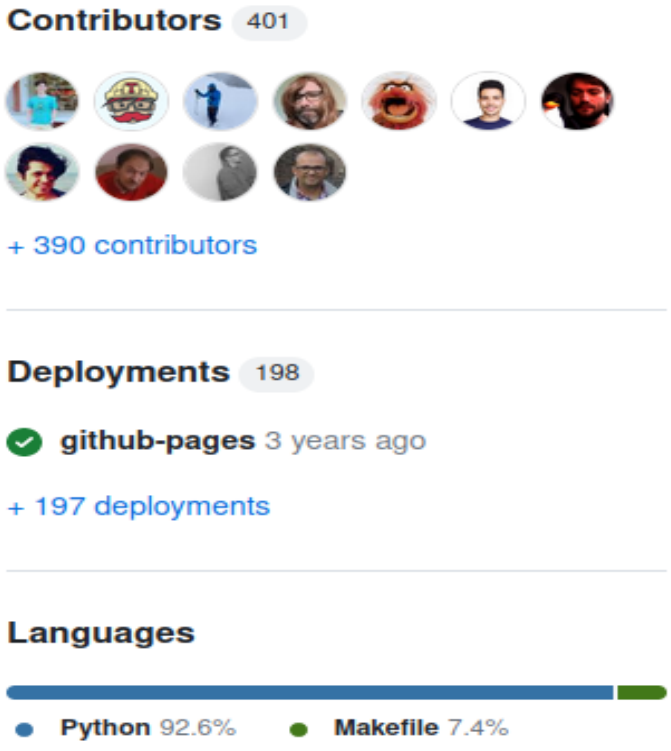
CI / CD Based

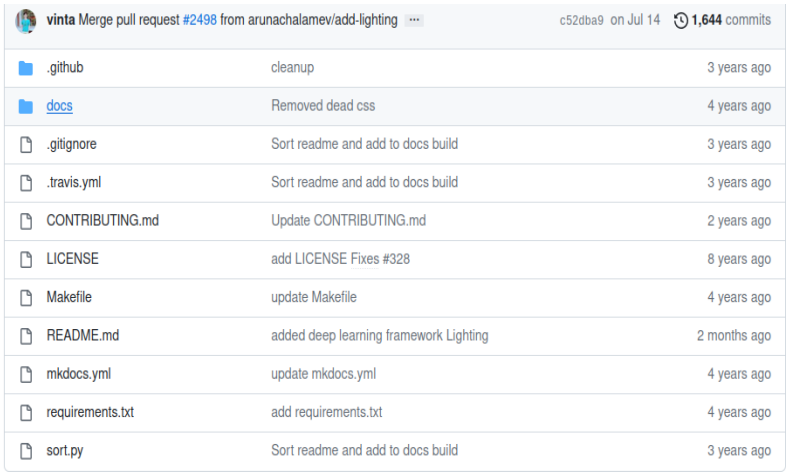
Introduce papers....

RESEARCH METHODS I

Data

- Fetch Data
- Clean Data





RESEARCH METHODS II

Framework

Introduce papers....

Pipeline

Introduce papers....

RESEARCH METHODS III

Metric

$$SM = (W_p \cdot P) * (W_{tf} \cdot TF) * (\frac{W_{tc}}{TC}) * (W_s \cdot S) \quad (1)$$

SM = Security Scanner Metric

P = Precision (as a decimal)

W_p = Weight for Precision

TF = Total Findings (TP + FP)

W_{tf} = Weight for Total Findings

TC = Time Cost

W_{tc} = Weight for Time Cost

S = Normalized Severity Score

W_s = Weight for Severity

SUMMARY

This is the first slide of your presentation.

REFERENCES I