Perception vs Reality

A Data-Driven Look at Open Source Risk Management

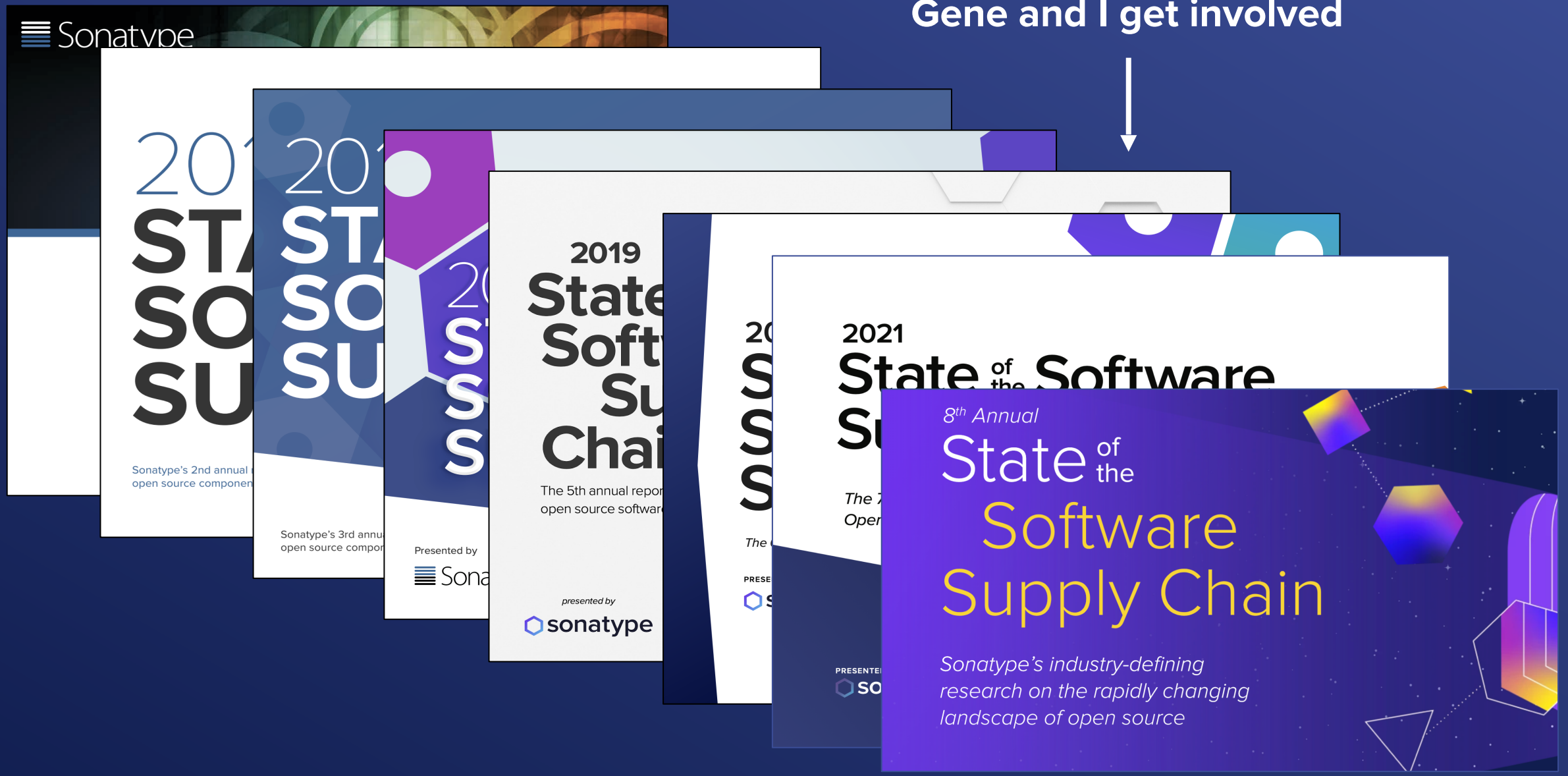
Dr. Stephen Magill

VP, Product Innovation

Sonatype

sonatype

Gene and I get involved



Production

Open Source Maintainers

Consumption

Enterprise Developers

Production

Perception: Open Source is risky

- 35% of releases are vulnerable (Maven Central)
- 3.5M vulnerable releases
- 1.2B vulnerable downloads per month

Reality: OSS Can Almost Always Be Secure

- 96% of projects have safe versions available
- Most vulnerabilities are patched before they’re disclosed
- Log4j: Patched in 15 days. Patch was available by the time the CVE went public.

Consumption

Perception: We're good at managing open source

- 68% are confident they are not using vulnerable versions
- High remediation maturity (self-reported)

Reality: Mixed Results

- 68% of applications use a component with a known vulnerability.
- Managers: 3.5x more likely to say remediation is fast (< 1 day)

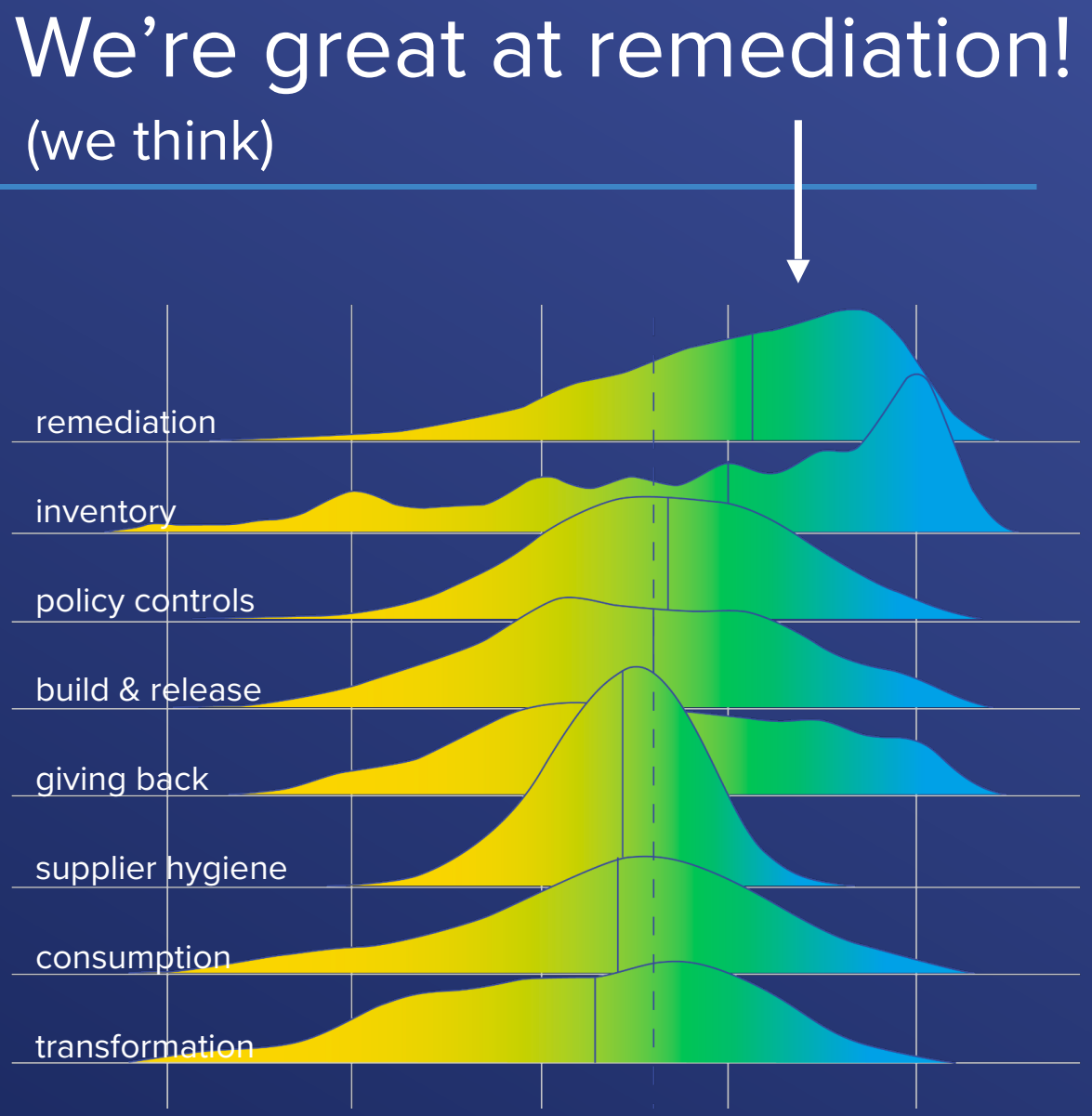


FIGURE 3.10. ENTERPRISE RESPONSE OVER TIME OF CRITICAL VULNERABILITIES BASED ON MEDIA COVERAGE

Producers

1.18 billion avoidable vulnerable versions each month

Consumers

sonatype

150 Dependencies (avg Java project)

x 10 Releases Per Year (avg per dependency)

1500 Updates To Consider 😱

Picking Better Components

Where better = “less likely to have a vulnerability”

OpenSSF Security Scorecard

Code Review
License File
Branch Protection
Pinned Dependencies
Official Packaging

Security Policy
Signed Releases
No Binaries
Active Commits
Safe Workflows

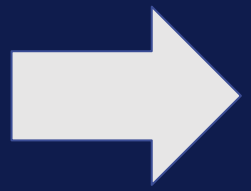
Update Tool
Workflow Permissions
Fuzz Testing
No Unpatched Vulns
Best Practices Badge

Connection With Security

OpenSSF Scorecard

Code Review	Security Policy	Update Tool
License File	Signed Releases	Workflow Permissions
Branch Protection	No Binaries	Fuzz Testing
Pinned Dependencies	Active Commits	No Unpatched Vulns
Official Packaging	Safe Workflows	Best Practices Badge

Machine Learning

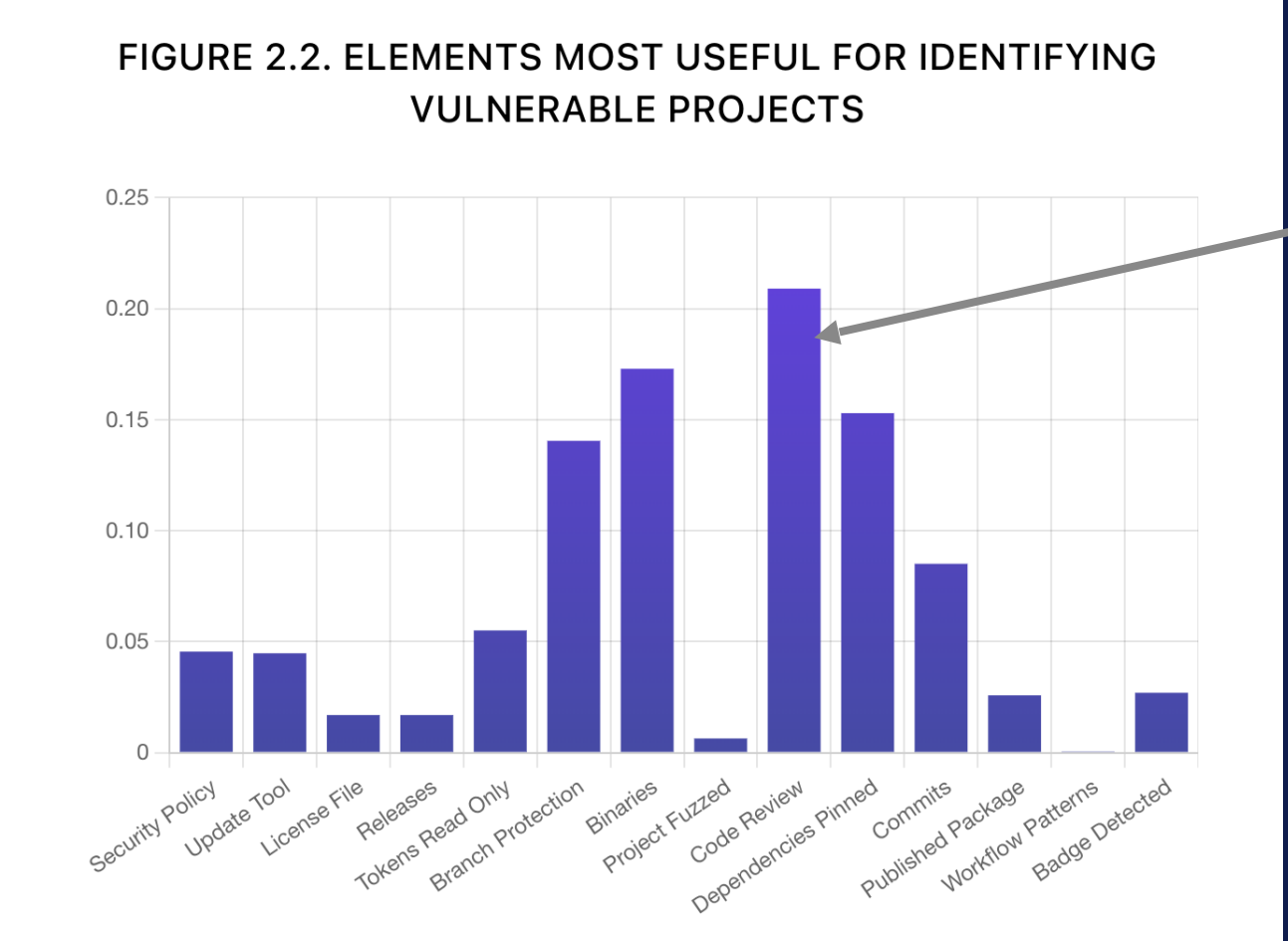


Predict whether a project has a known vulnerability

Can do this with 78% accuracy

What Is Most Important?

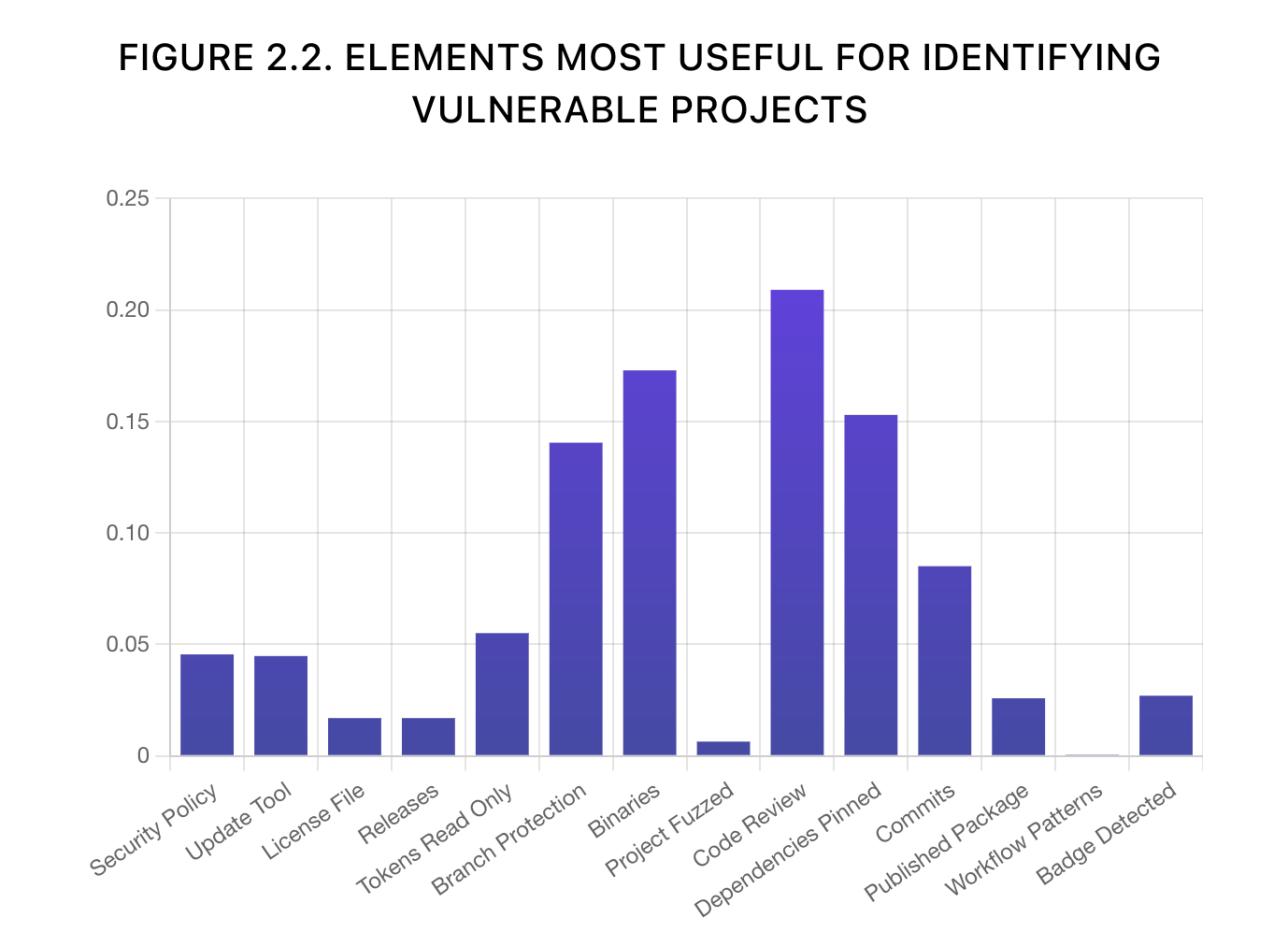
OpenSSF Scorecard



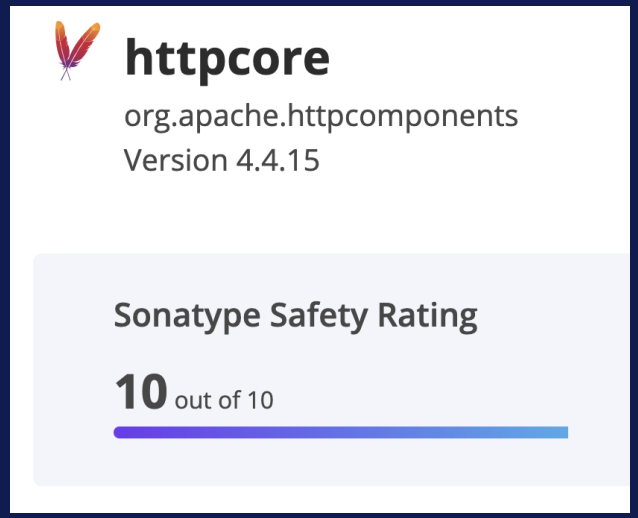
Most Important: Code Review

Converting To A Rating

OpenSSF Scorecard

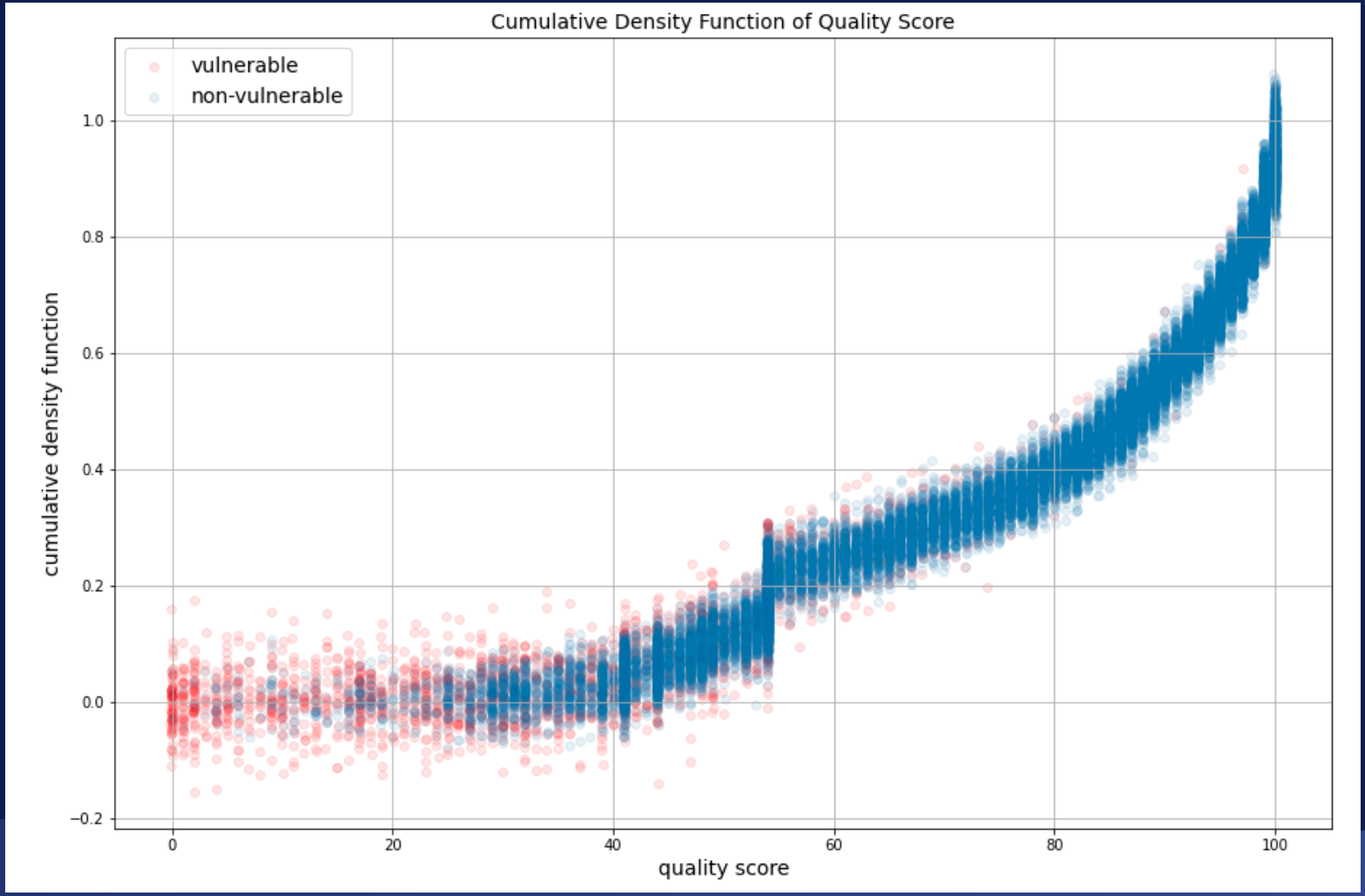


+ Dependency Hygiene Rating (MTTU)



Sonatype Safety Rating

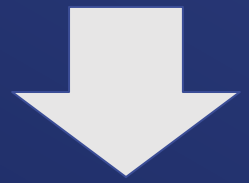
Not Perfect: 86% Accuracy



sonatype

Production

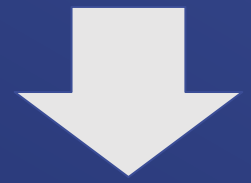
Open Source Maintainers



- Implement Scorecard Best Practices
- Keep Dependencies Up-to-date

Consumption

Enterprise Developers



- Choose projects with a high Safety Rating
  (and help us make it better)
- Use tools to flag and fix vulnerable libraries
- Get a realistic view of your organization’s performance