



Bitergia



Analyzing Risk from an OSS Project Health Perspective: **Tools, Traces, and Threats**

CHAOSScon EU 2025, Brussels, Belgium - Jan. 30, 2025

Georg Link, PhD

Meet Georg Link

Open Source Strategist

- Business focus
- 20+ years in open source
- Co-Founder of CHAOSS
- Community Builder



"My mission is to improve the health and sustainability of open source."

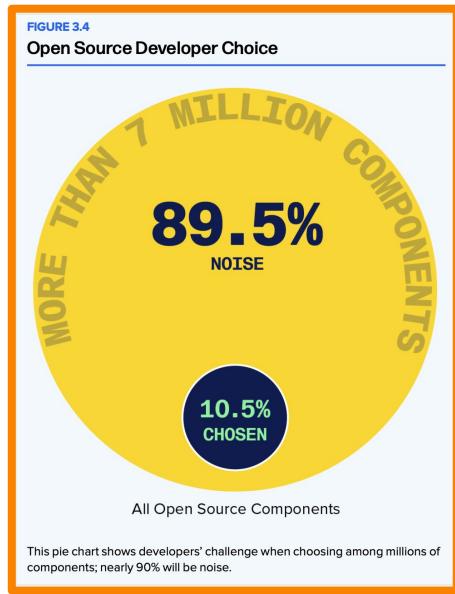


Threats

Open Source Today



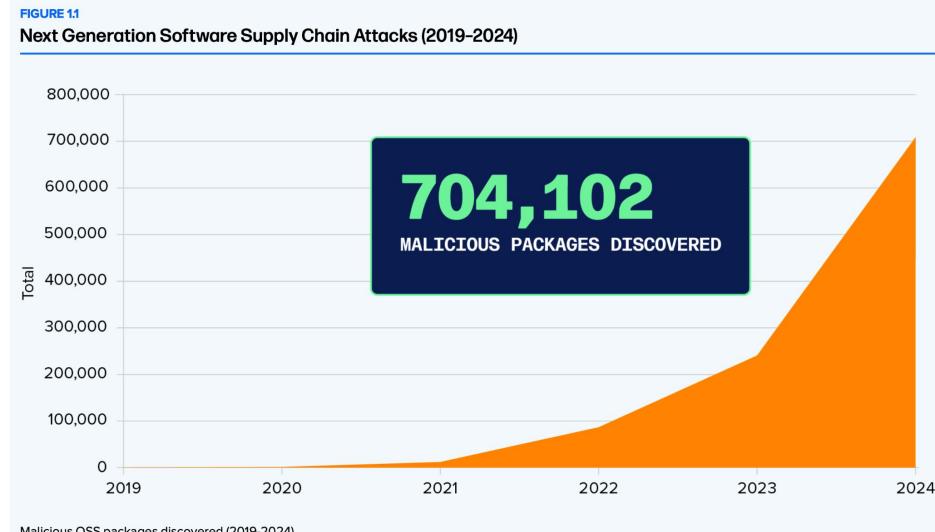
Dilemma: Choice and Maintenance



<https://www.sonatype.com/state-of-the-software-supply-chain>

Sonatype 9th State of Software Supply Chain report:
“Consider this: last year, we revealed that a staggering **85% of projects in Maven Central** – the largest public repository for Java open source components – **are inactive**. In other words, developers are faced with a perplexing array of choices, with only a fraction of them leading to active, well-maintained projects.”

Software Supply Chain Attacks are on the Rise

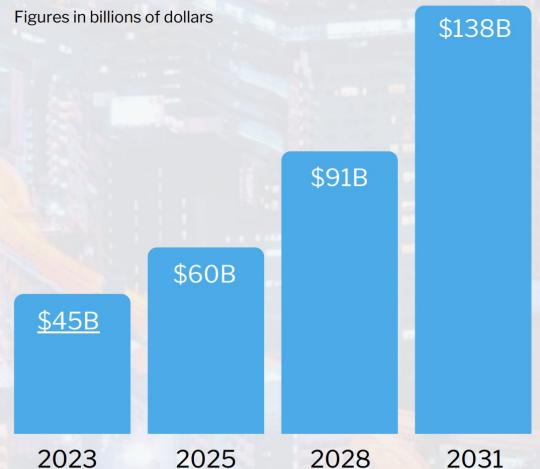


Software Supply Chain Attacks are on the Rise

DAMAGE COSTS

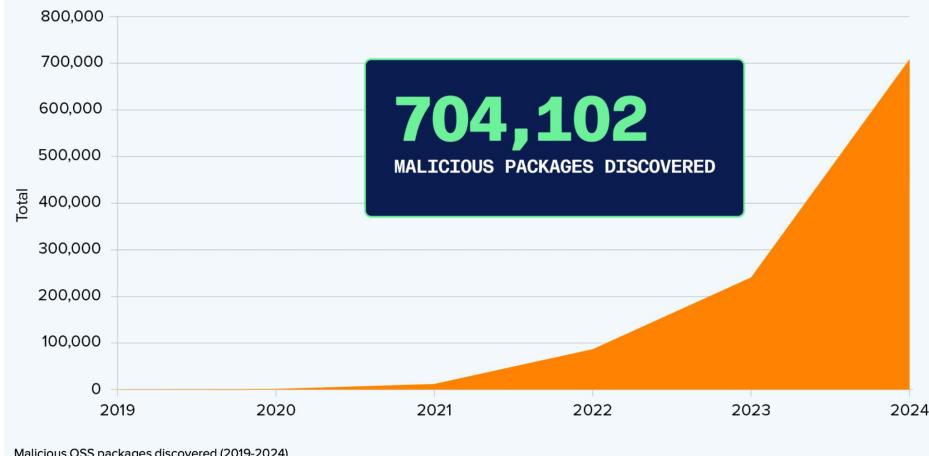
Cybersecurity Ventures predicts that the global cost of software supply chain attacks to businesses will reach nearly \$138 billion by 2031, up from \$60 billion in 2025, based on 15 percent year-over-year growth.

Figures in billions of dollars



<https://go.snyk.io/2023-supply-chain-attacks-report.html>

FIGURE 1.1
Next Generation Software Supply Chain Attacks (2019-2024)



<https://www.sonatype.com/state-of-the-software-supply-chain>

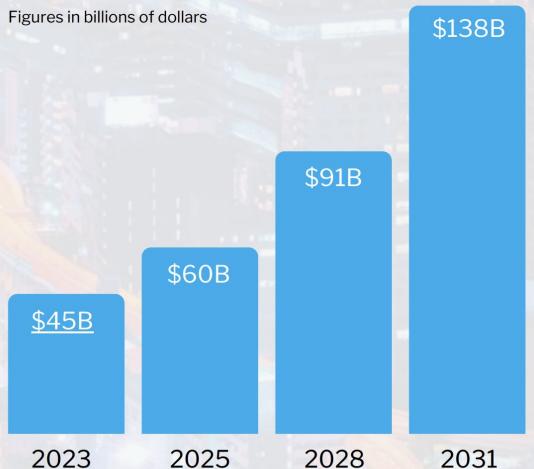


Software Supply Chain Attacks are on the Rise

DAMAGE COSTS

Cybersecurity Ventures predicts that the global cost of software supply chain attacks to businesses will reach nearly \$138 billion by 2031, up from \$60 billion in 2025, based on 15 percent year-over-year growth.

Figures in billions of dollars

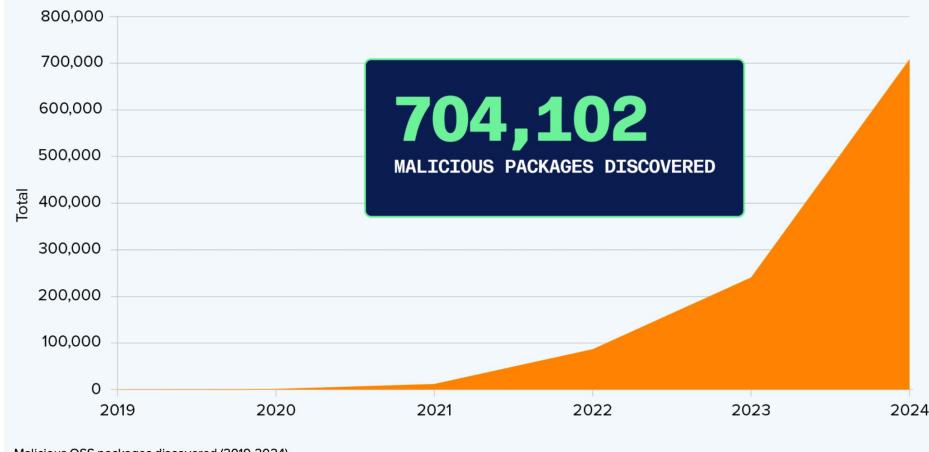


<https://go.snyk.io/2023-supply-chain-attacks-report.html>

Gartner predicts that by 2025, **45 percent** of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021.

([Gartner, Mar 7, 2022](#))

FIGURE 1.1
Next Generation Software Supply Chain Attacks (2019-2024)



<https://www.sonatype.com/state-of-the-software-supply-chain>



**Research Found the
SolarWinds Cyber Attack Cost**

Affected Companies in Key Sectors

11% of Total Annual Revenue

on Average

Results indicate cyber-related information sharing is increasing, signaling a positive response to national-and industry-level calls to action

By Business Wire

Jun 28, 2021

Traces

SBOM & Trust



Software ages like Milk, not Wine



Trust: Expiration Label and Source Information



Cyber Resilience Act (CRA)

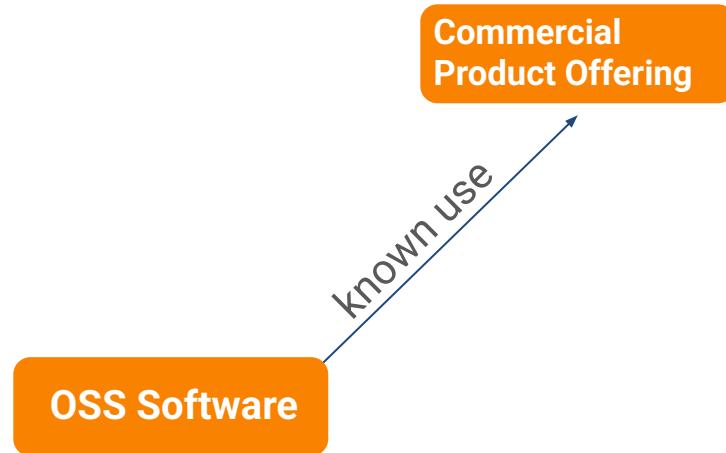
- (34) When integrating components sourced from third parties in products with digital elements during the design and development phase, manufacturers should, in order to ensure that the products are designed, developed and produced in accordance with the

**When integrating components sourced from third parties ...
manufacturers should, ... exercise due diligence with regard to
those components, including free and open-source software
components ...**

the market and for the support period, apply to products with digital elements in their entirety, including to all integrated components. Where, in the exercise of due diligence, the manufacturer of the product with digital elements identifies a vulnerability in a component, including in a free and open-source component, it should inform the person or entity manufacturing or maintaining the component, address and remediate the vulnerability, and, where applicable, provide the person or entity with the applied security fix.

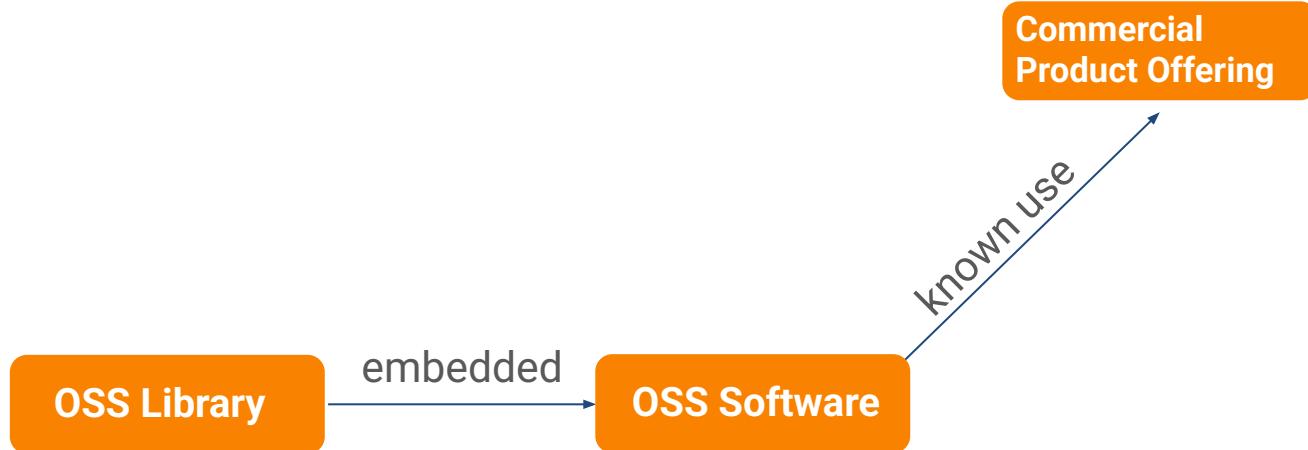
Context: Unmanaged OSS Use → Unknown Risk

- Developers use open source software
- 70% - 95% of software includes open source



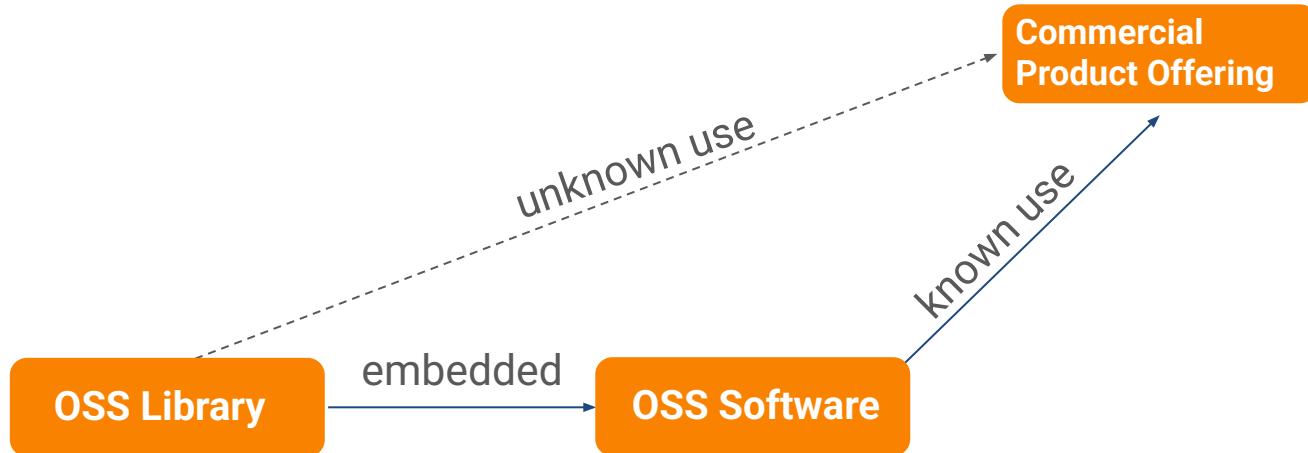
Context: Unmanaged OSS Use → Unknown Risk

- Developers use open source software
- 70% - 95% of software includes open source
- Unmanaged OSS use → unknown dependencies



Context: Unmanaged OSS Use → Unknown Risk

- Developers use open source software
- 70% - 95% of software includes open source
- Unmanaged OSS use → unknown dependencies → **unknown risk**



Software Bill of Material (SBOM)

An SBOM is a nested inventory,
a list of ingredients that make up
software components.

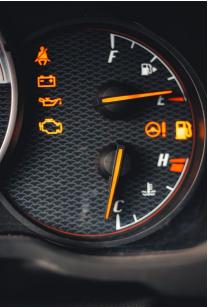


Imagine a Car

State Today:

- Flat Tires
- No Gas
- Warning Symbols
- Error Codes

→ You know how to fix today's situation



Risk - future support:

- Availability of Replacement Parts
- Skilled Workers to Repair
- Network of Repair shops
- Life Expectancy of Car

→ Unsupported Oldtimer vs. Supported Modern Car



Imagine a Car

State Today:

- Flat Tires
- No
Gas
- Water
Leak
- Engine
Failure

Licenses

Vulnerabilities

→ You know your car's current situation



Risk - future support:

- Availability of Replacement Parts
- Skilled Workers to Repair
- Network of Repair shops
- Life Expectancy of Car

→ Unsupported Oldtimer vs. Supported Modern Car



Imagine a Car

State Today:

- Flat Tires
- No
● Water
● Err

Licenses

Vulnerabilities

→ You know your situation



Risk - future support:

- Availability of Replacement Parts
- Skill Level of Driver
- Network of Support
- Life Expectancy of Vehicle

Under-maintained projects

→ Unsupported Modern Car



Problem: Trust in OSS Libraries to Manage Risk

Licenses

Vulnerabilities

Under-maintained projects



Problem: Trust in OSS Libraries to Manage Risk

Licenses

- License scanners

Vulnerabilities

- Software Composition Analysis (SCA)
- Vulnerability Databases

Under-maintained projects

180

average number of components
per application | **EVEN SMALL APPLICATIONS**
FACE UNMANAGEABLE WORKLOADS

<https://www.sonatype.com/state-of-the-software-supply-chain>



Problem: Trust in OSS Libraries to Manage Risk

Licenses

- License scanners

Vulnerabilities

- Software Composition Analysis (SCA)
- Vulnerability Databases

Under-maintained projects

- Community Health Metrics (CHAOS)
- Pay for support



Missing: Forward looking risk



Community Traces Indicate Health



The community activity today is a leading indicator for the software project's future.



Tools

The Role of CHAOSS



Indicators for Risk: “Under-maintained Projects”

CHAOSS metrics that scale, include 7 metrics:

Community cannot handle workload

- Backlog Management Index
- Review Efficiency Index

Community does not address work quickly

- Median Lead Time for Issues
- Median Lead Time for Pull Requests

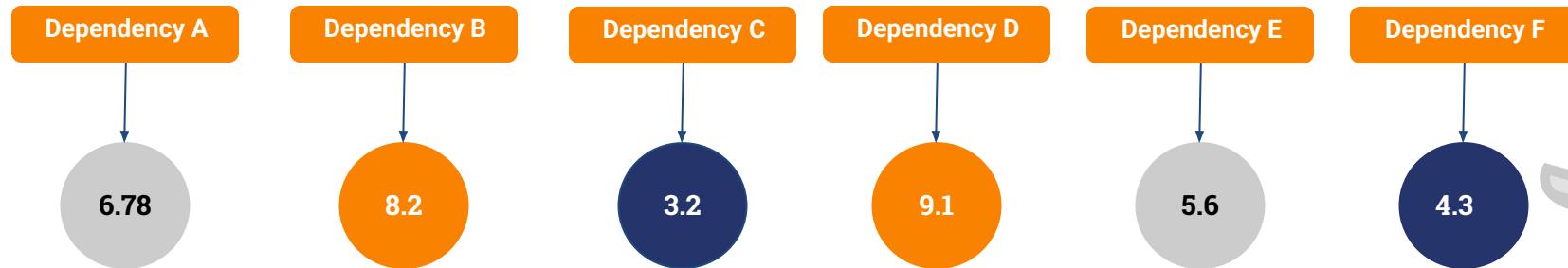
Community lacks sufficient talent

- Retention Rate
- Growth of Active Contributors
- Contributor Absence Factor (aka Bus or Pony Factor)

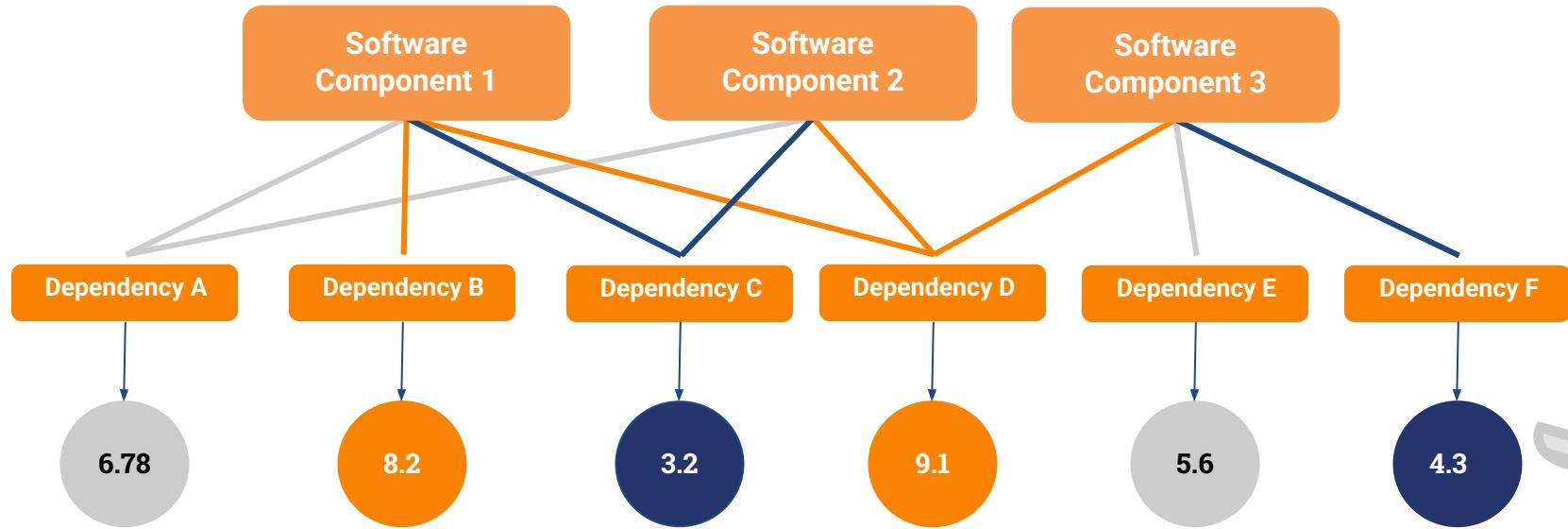


A single Risk Score per OSS library

7 metrics, normalized, and
combined into one score for each dependency



Risk Model - Aggregate By Component



Prototype:

Example of Kubernetes' Go Dependencies

project: Kubernetes - Golang Deps Add filter

Risk Model Overview Dashboard

Check the [Risk Model Help Dashboard](#) for more information about this analysis.

For more details, pin a filter by origin and visit the [Risk Model Dashboard for Individual Projects](#).

Filters

Team

Project Category

Overview

347

Dependencies analyzed

Bitergia
Team

Risk Value per Metric, by number of Dependencies

	89	191	67	17 - 79
BMI	89	191	67	79 - 141
Growth of Active Contributors	45	46	256	141 - 203
Median Lead Time for Issues	86	196	65	203 - 264
Median Lead Time for PRs	152	17	178	
Pony Factor	21	62	264	
REI	148	25	174	
Retention Rate	81	42	224	
	low	medium	high	
				Individual Metric Risk Value

Dependencies by Risk value

Dependencies



Overall results by dependency repository

Filter...



Repository	Category	Risk Value	Risk Score (over 10)	# "Low risk" metrics	# "Medium risk" metrics	# "High risk" metrics	Last analyzed on
https://github.com/json-iterator/go	Kubernetes - Golang Deps	very high	10	0	0	7	Jun 27, 2024 @ 12:35
https://github.com/spf13/afero	Kubernetes - Golang Deps	very high	10	0	0	7	Jun 27, 2024 @ 12:35
https://github.com/Azure/go-anisitern	Kubernetes - Golang Deps	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35
https://github.com/Thalesignite/crypto11	Kubernetes - Golang Deps	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35
https://github.com/coreos/go-semver	Kubernetes - Golang Deps	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35
https://github.com/curioswitch/go-reassign	Kubernetes - Golang Deps	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35
https://github.com/davecgh/go-spew	Kubernetes - Golang Deps	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35

Export: Raw Formatted

project: Kubernetes - Golang Deps × Add filter

Risk Model Overview Dashboard

Check the [Risk Model Help Dashboard](#) for more information about this analysis.

For more details, pin a filter by origin and visit the Project Category page.

Filters

Team

Select...

Project Category

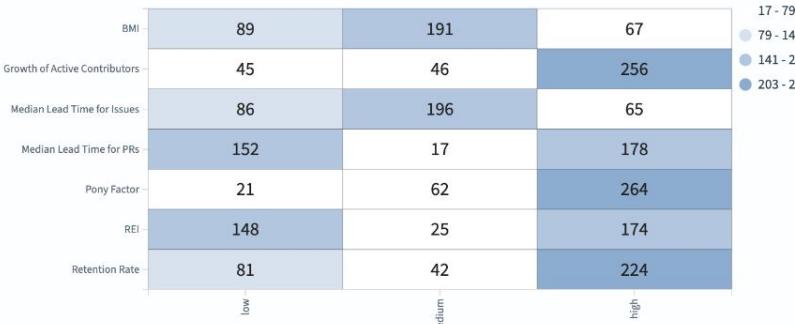
Kubernetes - Golang Deps ×

Project Category

Kubernetes - Golang Deps ×



Risk Value per Metric, by number of Dependencies



Dependencies by Risk value

Dependencies

very high 131

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

low

medium

high

very high

high

medium

low

very low

project: Kubernetes - Golang Deps X Add filter

Risk Model Overview Dashboard

- Check the [Risk Model Help Dashboard](#) for more information about this analysis.
- For more details, pin a filter by origin and visit the [Risk Model Dashboard for Individual Projects](#).

Filters Overview

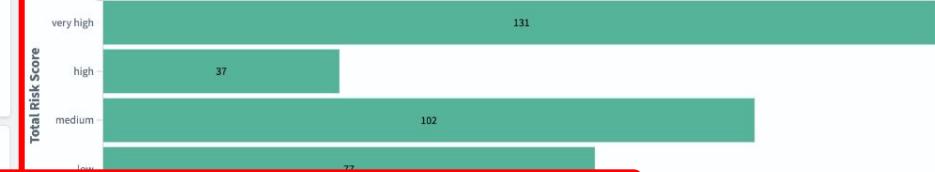
Dependencies by Risk value

Dependencies



Dependencies by Risk value

Dependencies



100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

100 120

Risk Model Overview

[Check the Risk Model Here](#)

For more details, pin a

Filters

Team

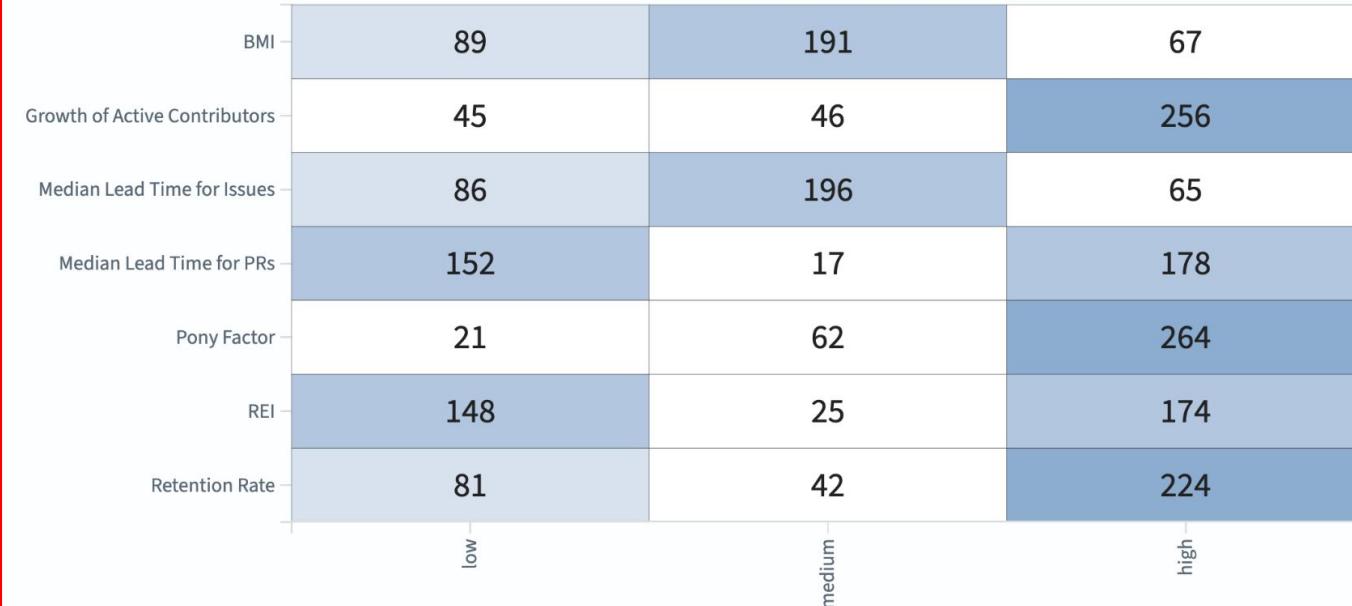
Select...

Project Category

Kubernetes - Golang Deps X

Risk Value per Metric, by number

Risk Value per Metric, by number of Dependencies



Individual Metric Risk Value

	low	medium	high
BMI			
Growth of Active Contributors			
Median Lead Time for Issues	86	196	65
Median Lead Time for PRs	152	17	178
Pony Factor	21	62	264
REI	148	25	174
Retention Rate	81	42	224

	Deps	Kubernetes - Golang	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35
https://github.com/coreos/go-semver	Deps	Kubernetes - Golang	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35
https://github.com/curiouswitch/go-reassign	Deps	Kubernetes - Golang	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35
https://github.com/davecgh/go-spew	Deps	Kubernetes - Golang	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35
Export: Raw Formatted								

project: Kubernetes - Golang Deps X Add filter

Risk Model Overview Dashboard

Check the [Risk Model Help Dashboard](#) for more information about this analysis.

For more details, pin a filter by origin and visit the [Risk Model Dashboard for Individual Projects](#).

Filters

Team

Select...

Project Category

Kubernetes - Golang Deps X

Risk Value per Metric, by number of Dependencies

	low	medium	high
BMI	89	191	67
Growth of Active Contributors	45	46	256
Median Lead Time for Issues	86	196	65
Median Lead Time for PRs	152	17	178
Pony Factor	21	62	264
REI	148	25	174
Retention Rate	81	42	224

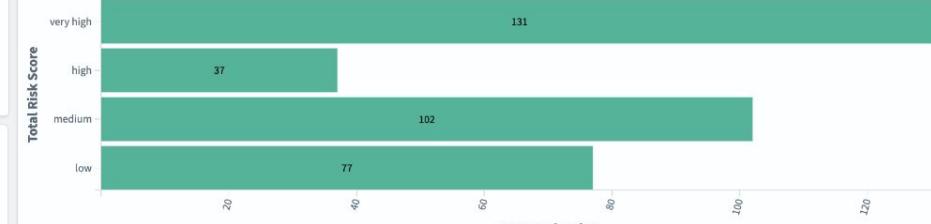
Individual Metric Risk Value

347
Dependencies analyzed

Drill Down

Dependencies by Risk value

Dependencies



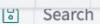
Overall results by dependency repository

Filter...



Repository	Category	Risk Value	Risk Score (over 10)	# "Low risk" metrics	# "Medium risk" metrics	# "High risk" metrics	Last analyzed on
https://github.com/json-iterator/go	Kubernetes - Golang Deps	very high	10	0	0	7	Jun 27, 2024 @ 12:35
https://github.com/spf13/afero	Kubernetes - Golang Deps	very high	10	0	0	7	Jun 27, 2024 @ 12:35
https://github.com/Azure/go-anisitern	Kubernetes - Golang Deps	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35
https://github.com/Thalesignite/crypto11	Kubernetes - Golang Deps	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35
https://github.com/coreos/go-semver	Kubernetes - Golang Deps	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35
https://github.com/curiouswitch/go-reassign	Kubernetes - Golang Deps	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35
https://github.com/davecgh/go-spew	Kubernetes - Golang Deps	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35

Export: Raw Formatted



project: Kubernetes - Golang Deps × origin: https://github.com/stretchr/testify × [+ Add filter](#)

Risk Model Dashboard for Individual Projects

Make sure to filter by a given repository before using this dashboard.

Check the [Risk Model Help Dashboard](#) for more information about this analysis.

[Go back to the Risk Model Overview Dashboard.](#)

Total Risk Score

github.com/stretchr/testify

Package Name

medium

Total Risk

4.29

Total Risk Score (over 10)

https://github.com/stretchr/testify

Package Repository

Select an dependency first to check its risk

Team

Select...

Dependency Pkg Name

Select...

Dependency Repository

Select...

Project Category

Kubernetes - Golang Deps ×



Risk Model: Detailed view - dependency selector table

stre



Dependency

<https://github.com/stretchr/testify>

Package Name

github.com/stretchr/testify

Risk Level

medium

Risk Score

4.29



Metric

Retention Rate

Risk Value

low

Metric Value

1.769

REI

low

1.164

Pony Factor

medium

2

Median Lead Time for PRs

high

90.285

Median Lead Time for Issues

high

221.23

Growth of Active Contributors

medium

0.833

BMI

low

1.337

Export: Raw Formatted

Export: Raw Formatted

Risk Model Dashboard for Individual Projects

- Make sure to filter by a given repository before using this dashboard.
- Check the [Risk Model Help Dashboard](#) for more information about this analysis.
- [Go back to the Risk Model Overview Dashboard.](#)

Total Risk Score

github.com/stretchr/testify

Package Name

medium

Total Risk

4.29

Total Risk Score (over 10)

<https://github.com/stretchr/testify>

Package Repository

Select an dependency first to check its risk

Team	Dependency Pkg Name	Dependency Repository	Project Category
Select...	Select...	Select...	Kubernetes - Golang Deps ×

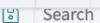
Risk Model: Detailed view - dependency selector table ⓘ

stre			
Dependency	Package Name	Risk Level	Risk Score
https://github.com/stretchr/testify	github.com/stretchr/testify	medium	4.29

Export: Raw Formatted

Metric	Risk Value	Metric Value
Retention Rate	low	1.769
REI	low	1.164
Pony Factor	medium	2
Median Lead Time for PRs	high	90.285
Median Lead Time for Issues	high	221.23
Growth of Active Contributors	medium	0.833
BMI	low	1.337

Export: Raw Formatted

**Metric**

Retention Rate

Risk Value

low

Metric Value

1.769

REI

low

1.164

Pony Factor

medium

2

Median Lead Time for PRs

high

90.285

Median Lead Time for Issues

high

221.23

Growth of Active Contributors

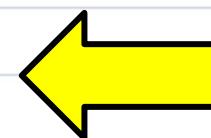
medium

0.833

BMI

low

1.337

**Dependency** <https://github.com/stretch/testify>**Package Name** github.com/stretch/testify**Risk Level**

medium

Risk Score

4.29

Dependency	Package Name	Risk Level	Risk Score
https://github.com/stretch/testify	github.com/stretch/testify	medium	4.29
REI		low	1.164
Pony Factor		medium	2
Median Lead Time for PRs		high	90.285
Median Lead Time for Issues		high	221.23
Growth of Active Contributors		medium	0.833
BMI		low	1.337

Export: Raw Formatted

Export: Raw Formatted

Experience



CHAOSS Expert Guide **is in the works**

Food for discussion,
additional metrics we could consider:

- licenses
- known vulnerabilities
- origin of developers
- organizational diversity





GrimoireLab: The Open Source Tool

Story of GrimoireLab

- 2004 LibreSoft @ University Rey Juan Carlos in Spain
- 2012 Bitergia offers commercial services with Metrics Grimoire
- 2016 GrimoireLab starts, using ElasticSearch for Dashboarding
- 2017 Founding of CHAOSS
- 2024 version 1.0 released



Example: Mozilla Foundation

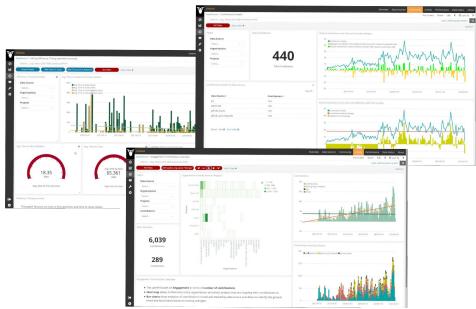


[...] holistic view of our contributor ecosystem's network structure, health and impact [...]

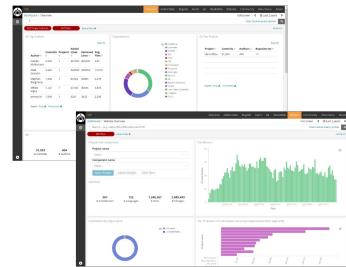
[...] we're able to visually describe these distinct contributor communities as well as how they are interconnected [...]

<https://report.mozilla.community/>

Platforms built with GrimoireLab



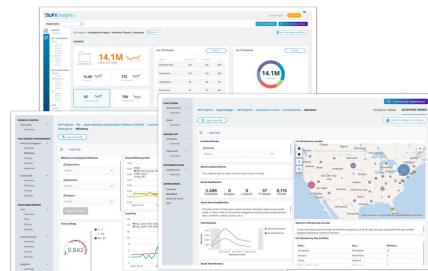
Bitergia Analytics



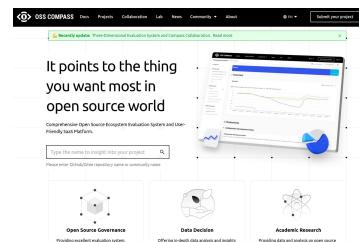
The Document Foundation



Mystic



Linux Foundation Insights



OSS Compass



Collecting traces from OSS communities

Data Collection

Traces: digital footprints
from data source

(biased towards activities
that are logged)



Enrichment

Translate data into
information

(connect and unify
for consistency)



Visualization and Reporting

Gain insights and decide
actions

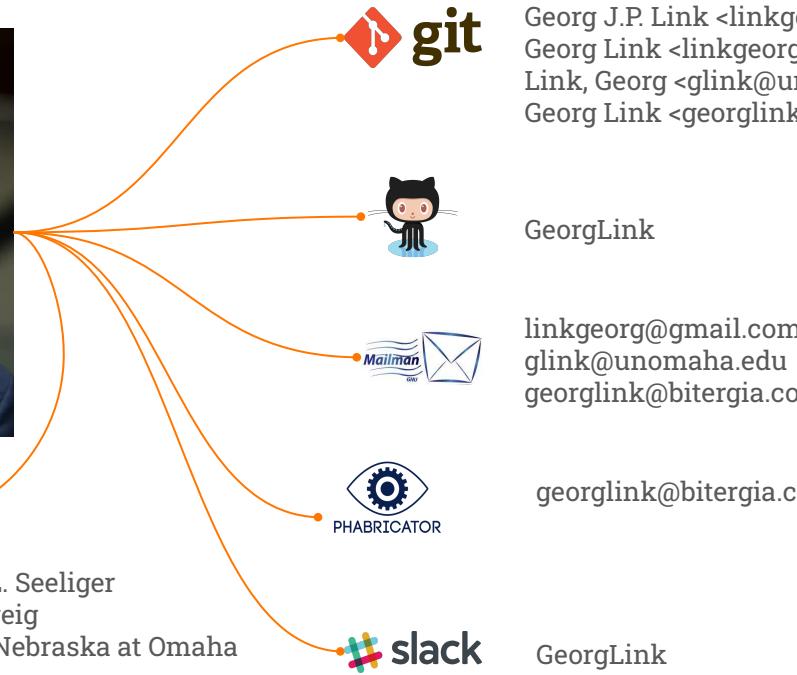
(tell stories and
convince)



SortingHat to disambiguate contributors



08/2008 - 07/2011 Bankhaus C. L. Seeliger
10/2011 - 05/2015 TU Braunschweig
08/2015 - 05/2019 University of Nebraska at Omaha
05/2019 - now Bitergia



Georg J.P. Link <linkgeorg@gmail.com>
Georg Link <linkgeorg@gmail.com>
Link, Georg <glink@unomaha.edu>
Georg Link <georglink@bitergia.com>

GeorgLink

linkgeorg@gmail.com
glink@unomaha.edu
georglink@bitergia.com

georglink@bitergia.com

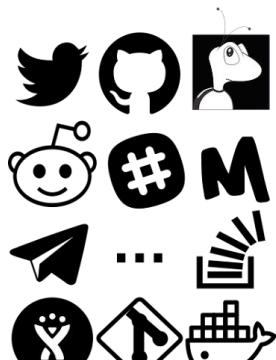
GeorgLink



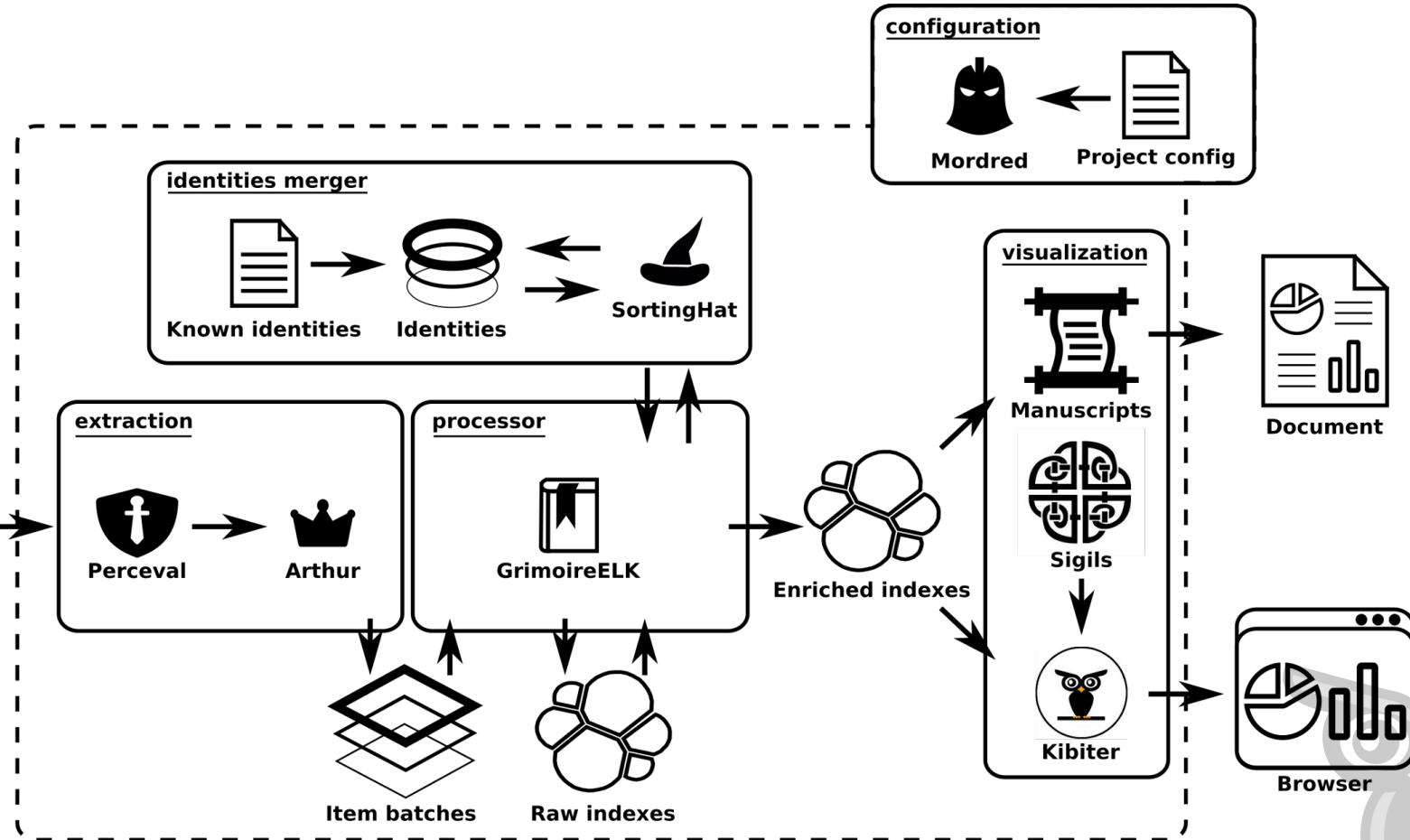
Excursion: Minding data privacy

- GDPR is gold standard
- Opt-in vs. Opt-out
- Enriching data from data sources
- Offering a “remove my data” feature





Data sources



GrimoireLab 2.0 roadmap

- **Maintenance effort:**  Graphical user interface and an API for configuring data collection
- **Scalability and performance:**  Currently, 3,500 high-active repositories require three days of data analysis before the data is ready for the user
- **Integration with other tools:**  Support more tools for visualizing and analyzing the data



How to Get Started?

Open Source: GrimoireLab tutorial

- <https://chaoss.github.io/grimoirelab-tutorial/>



Commercial Support: Bitergia Analytics

- <https://bitergia.com/bitergia-analytics/>

Thank you and please reach out!

CHAOScon EU 2025
Brussels, Belgium
Jan. 30, 2025



Georg Link, PhD
georglink@bitergia.com

FOSDEM:

- * DevRoom: Funding the FOSS Ecosystem on Sunday at 9:10.
- * DevRoom: SBOM on Sunday at 15:30.