

SBOM Play



SBoM Exploration and Intelligence extraction platform

By

Anant Shrivastava
Cyfinoid Research

SBOM Play



- SBOM Exploration and intelligence extraction platform
- IN-Browser
- Fully client side

Core Idea



- SBOM is just an inventory
- Using SBOM in non-infosec scenarios
- Showing is better than talking

One Field : As simple as it can get



[Home](#) [License](#) [Vulns](#) [Audit](#) [Findings](#) [Insights](#) [Agent](#) [Deps](#) [Repos](#) [Authors](#) [Settings](#) [About](#) 



Analyse SBOMs from a GitHub org, user, repo, or URL — all in your browser.

Presented @ [BlackHat](#)

Presented @ [Defcon](#)

Launched @ [Peerlist](#)

 [Sponsor](#) 

 [Buy Me A Coffee](#)

 All analysis happens in your browser. No data is sent to any server.

 [GitHub](#)

 Upload SBOM

Enter a GitHub organization, username, repository, or URL to analyze*

e.g., microsoft, torvalds, microsoft/vscode, or https://github.com/cyfinoid/sbomplay

 Start Analysis

 Optional: GitHub token for higher rate limits



Information Classification: General

black hat
USA
2026

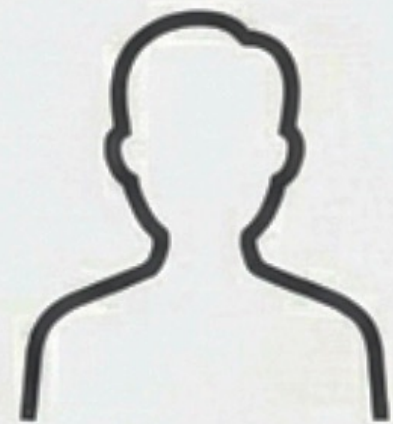
4

SBoM Play: Input



- A Github organization / user / repository
 - Either in shortform user/repo or org/repo or username or org
 - Or full github url <https://github.com/cyfinoid/sbomplay>
-
- P.S. We just need Dependency Graph enabled on repositories.

Under the hood



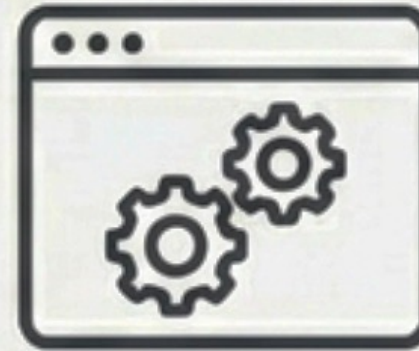
1. INPUT

User provides a GitHub Org, User, or Repo URL.



2. FETCH

The browser queries the GitHub Dependency Graph API for SBOM data.



3. RESOLVE & AUGMENT

The in-browser engine resolves the full dependency tree by querying public registries (npm, PyPI, etc.) and vulnerability databases (OSV.dev).



4. ANALYZE & VISUALIZE

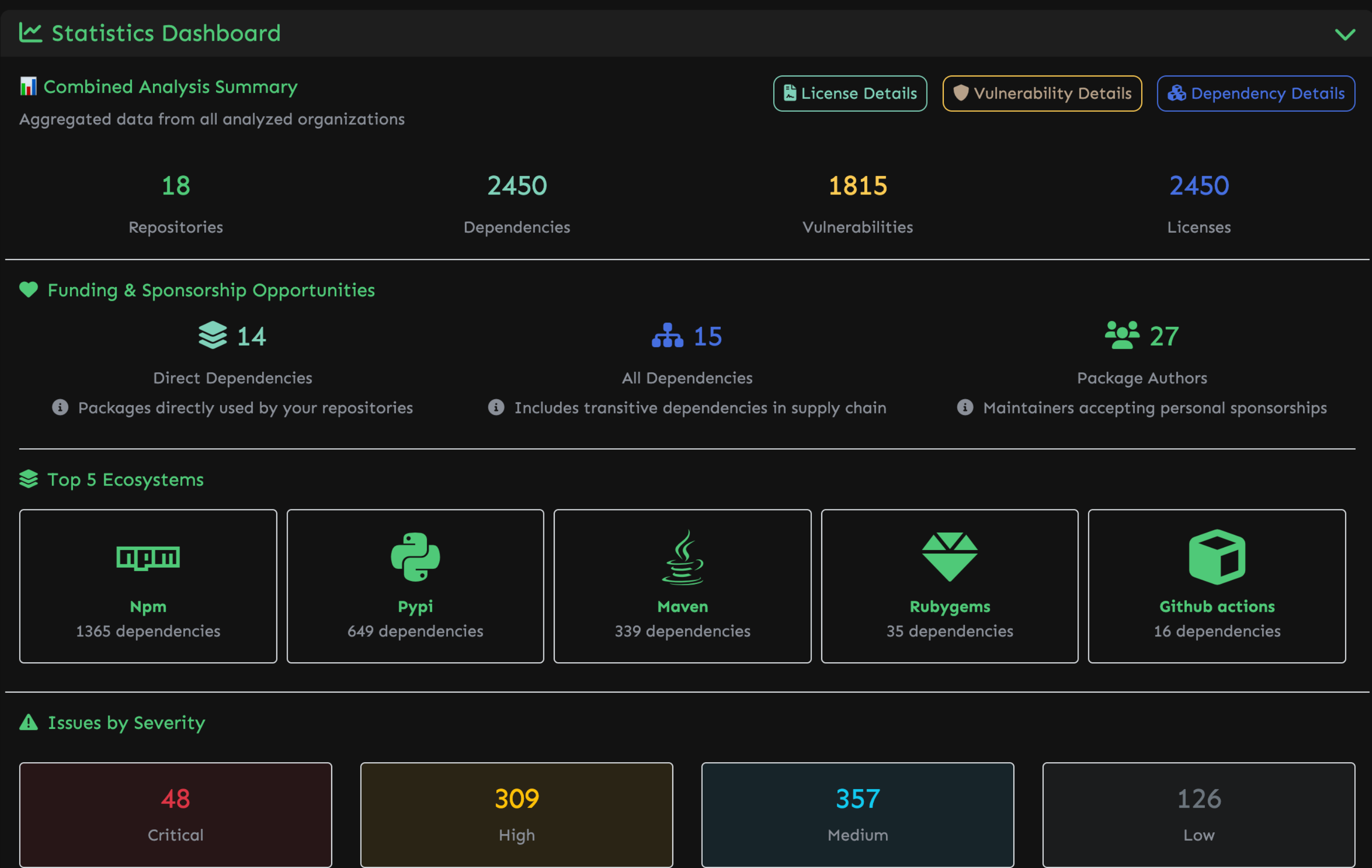
Results are processed and displayed across multiple interactive views.



5. STORE

All analysis data is stored locally in the browser's IndexedDB for persistence.

Dashboard 10k feet view



Version Sprawl



Top 5 Dependencies with Version Sprawl

org.slf4j:slf4j-api

10 versions

Version Sprawl

 View

Versions: 1.7.25, 1.7.29, 1.7.32, 1.7.36, 2.0.0-alpha1 ... and 5 more

flask

6 versions

Version Sprawl

 View

Versions: 1.1.2, 2.0.3, 2.2.5, 2.3.3, 3.1.3 ... and 1 more

org.apache.commons:commons-lang3

6 versions

Version Sprawl

 View

Versions: 3.1, 3.12.0, 3.13.0, 3.14.0, 3.16.0 ... and 1 more

org.codehaus.plexus:plexus-utils

6 versions

Version Sprawl

 View

Versions: 1.0.4, 1.5.5, 1.5.8, 3.0.17, 3.0.20 ... and 1 more

numpy

5 versions

Version Sprawl

 View

Versions: 1.19.5, 1.26.0, 1.26.4, 2.5.1, unknown

Top 5 Most common Dependencies



★ Top 5 Most Commonly Used Dependencies



certifi@2026.7.22

Used in 5 repositories

 View

idna@3.18.0

Used in 5 repositories

 View

colorama@unknown

Used in 4 repositories

 View

charset-normalizer@3.4.9

Used in 4 repositories

 View

urllib3@2.7.0

Used in 4 repositories

 View

Dependency View



Analysis

Search

Type

Ecosystem

Repository

All Analyses (2450 deps)

Search package name...

All

All

All

Vulnerable

Seeking sponsorship

Major drift

Minor drift

Unmaintained

End-of-life

2450

Total Dependencies

309

Direct

2141

Transitive

2450

Showing (filtered)

Dependencies

Export OPML

Export CSV

Dependency	Ecosystem	Repos	Vulns	License	Sponsor	Brought in by
@alloc/quick-lru@5.2.0	npm	1 repo	—	MIT	—	1 parent
@ampproject/remapping@2.3.0	npm	2 repos	—	Apache	—	1 parent
@apideck/better-ajv-errors@0.3.7	npm	1 repo	—	MIT	—	1 parent

Vulnerability View



apache-airflow@3.1.8 Transitive ↑ Minor: 3.3.0

75 vulnerabilities

UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN
UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN
UNKNOWN	UNKNOWN	MODERATE	HIGH	MODERATE	HIGH	MODERATE	MODERATE	MODERATE	CRITICAL	CRITICAL	MODERATE	
LOW	MODERATE	HIGH	MODERATE	MODERATE	HIGH	MODERATE	MODERATE	MODERATE	MODERATE	LOW	LOW	UNKNOWN
UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN
UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN
UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN						

[View Details](#)

🔗 Used in 1 repository:

sbomplay-demo/python-deep-deps: apache-airflow@2.8.0 → apache-airflow-providers-common-sql@1.20.0 → apache-airflow@2.11.2 → apache-airflow-providers-fab@1.5.4 → apache-airflow@3.1.8

Repository View



Analysis

All Analyses (18 repos)

Search

Search repository name...

Rows

25

18

Total Repositories

18

With SBOM

10

With Vulnerabilities

18

Showing (filtered)

☰ Repositories

📄 Export as CSV

License Compliance



License Compliance

License compatibility and risk assessment across your dependencies.

[← Back to Analysis](#)

Analysis

All Analyses (2450 deps)

License category

All categories

Reach

All

Unlicensed

86

unlicensed deps

Copyleft

22

high risk

Unknown

4

high risk

Proprietary

0

medium risk

Custom

6

needs review

Total

2364

licensed deps

License Changes

2

transitions

License Changes Detected

All license changes across all dependencies (not just high-risk)

Dependency	Version 1 @ License 1	Version 2 @ License 2	Repositories
------------	-----------------------	-----------------------	--------------

License Change



JUnit » 4.5

JUnit is a unit testing framework to write and run tests, organize, and execute automated tests, ensuring code quality and facilitate the development and running of test cases and test-driven development.

License	CPAL 1.0 CPL 1.0
Categories	Testing Frameworks & Tools
Tags	testing junit quality

[Home](#) » [junit](#) » [junit](#) » 4.12



JUnit » 4.12

JUnit is a unit testing framework to write and run tests, organize, and execute automated tests, ensuring code quality and facilitate the development and running of test cases and test-driven development.

License	EPL 1.0
Categories	Testing Frameworks & Tools
Tags	testing junit quality

Author Details on a map



Author Locations Map

 Hide Map

 Locations are self-reported by package authors; accuracy varies.



Author Details



i Showing 25 of 353 human authors from 7 ecosystems (238 with multiple packages, 115 with single package across multiple repos)

🔗 For packages whose source repository is on GitHub, the top 10 repository contributors are included as *tentative* authors (marked with **!** in the location column). When several packages share the same repository (e.g. monorepos like `spring-projects/spring-boot` or `babel/babel`), all of those packages will list the same contributors — that's the intended behaviour: a compromise of the shared repo affects every package that ships from it. Automated bots (Dependabot, Renovate, GitHub Actions, ...) are routed to the **Active Bots in the Environments** section below instead of the human authors list.

☰ Show All 353 Authors

#	Author	Ecosystem	Packages	Repository Usage		Location	Social	Sponsorship
1	Ian Stapleton Cordasco	pypi	4	4 repos	Moderate Risk	Virginia, USA, Earth, Milky Way. !		—
2	Lukasa	pypi	11	3 repos	Moderate Risk	London, England !		—
3	msabramo	pypi	8	3 repos	Moderate Risk	San Jose, California, USA !		—
4	mitsuhiko	cargo	7	3 repos	Moderate Risk	Austria !		—
5	siamavirus24	pypi	6	3 repos	Moderate Risk	Madison, WI !		—

SBoM Auditing



SBOM Audit

18/18

Repositories with SBOM

0

CISA 2025

18

Fresh SBOMs

54%

Avg Completeness

Grade Distribution

D: 18

CISA 2025: 0/18 (0%)
US Federal SBOM requirements

BSI TR-03183: 0/18 (0%)
German/EU technical guideline

CERT-In: 0/18 (0%)
Indian CERT guidelines

Repository SBOM Quality

Source	Repository	Format	Grade	Score	CISA	BSI	CERT	Freshness	Complete	Details
	sbomplay- demo/github-actions-nested	SPDX 2.3		5.1/10					44%	
	sbomplay- demo/github-actions-basic	SPDX 2.3		5.1/10					44%	

SBoM Enrichment Findings



Security Findings Summary



CRITICAL	Malware	Known Malicious Package	7 findings	✓
HIGH	EOX (End-of-Life/Support)	Highly Likely EOL (Abandoned)	323 findings	✓
HIGH	GitHub Actions	Mutable Tag Reference	42 findings	✓
HIGH	Dependency Confusion	Potential Dependency Confusion	6 findings	✓
HIGH	EOX (End-of-Life/Support)	End-of-Life (EOL)	6 findings	✓
MEDIUM	EOX (End-of-Life/Support)	Probable EOL	94 findings	✓
MEDIUM	EOX (End-of-Life/Support)	End-of-Support (EOS)	1 finding	✓

Insights



AI Agents coz why not



100% on-device AI — no server-side inference

This page uses Chrome's built-in **Gemini Nano** (Prompt API) on your machine. Your SBOM analysis, questions, and model answers are **not sent to SBOM Play or any cloud LLM**. SBOM data is read from local IndexedDB; only tool-query results in memory are summarized by the on-device model.

SBOM Analyst Agent

On-device Gemini Nano summarizes SBOM tool queries — nothing leaves your browser

● Gemini Nano (on-device) no cloud LLM queries: app-driven

All Analyses (2450 deps) ▾

+ New

18

REPOS

2450

DEPS

357

C+H VULNS

423

EOL

C

GRADE

How is our overall security posture?



QUERIES 4 queries · click to expand ▾

QUERY query_sbom(overview) ✓

QUERY query_sbom(techDebt) ✓

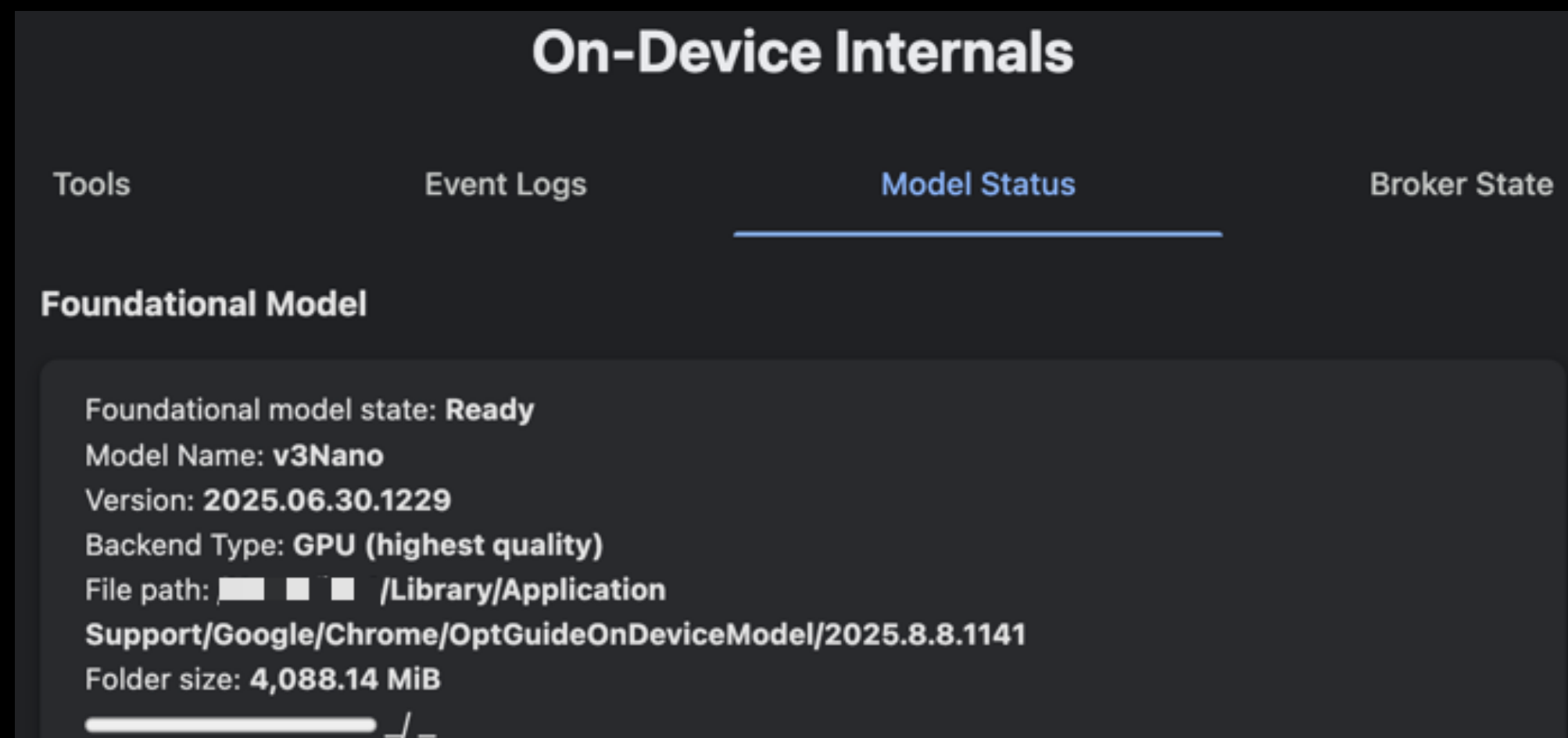
QUERY query_sbom(supplyChain) ✓

QUERY query_sbom(vulnerabilities, filter: critical) ✓

AI Agent under the hood



- Works only in Google Chrome
- Google Chrome now ships with inbuilt LLM
- So, all activities are happening in browser no network call



SBOMPlay in a nutshell



SBOM Play: SBOM Exploration and Intelligence Extraction Platform



Your SBOM Intelligence Hub - In Your Browser

Privacy-First by Design

All analysis happens locally in your browser; no data is ever sent to a server.

Input...



Simple Input, Powerful Insight

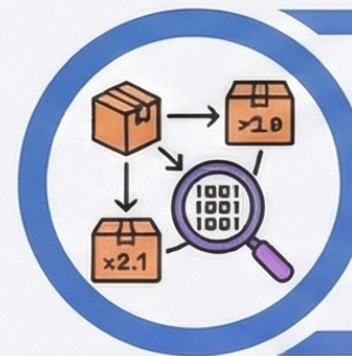
Just enter a GitHub organization, user, or repository URL to begin the analysis.



Multi-Ecosystem Support

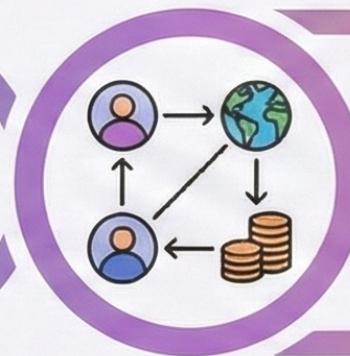
Tracks dependencies across npm, PyPI, Maven, Go, GitHub Actions, and more.

Go Beyond Vulnerability Scanning



Uncover Dependency Patterns

Identify commonly used packages and detect *version sprawl* across your projects.



Analyze Your Contributors

Identify third-party authors, visualize their locations, and discover funding opportunities.



Manage License Compliance

Assess license risks and automatically detect license changes between package versions.

Explore Your Supply Chain

Try It Now

<https://cyfinoid.github.io/sbomplay/>



A Product By **Cyfinoid Research**
cyfinoid.com

© NotebookLM

<https://github.com/cyfinoid/sbomplay>