



Commoditising Open Source Risk Management

First Open Source SCA Platform

Julian Coccia
CTO

KNOW YOUR FRANKIE

- 75% is Open Source

The Forrester Wave™,
Software Composition Analysis
Q3 2021

- 85-90% is Open Source

Github, 2022



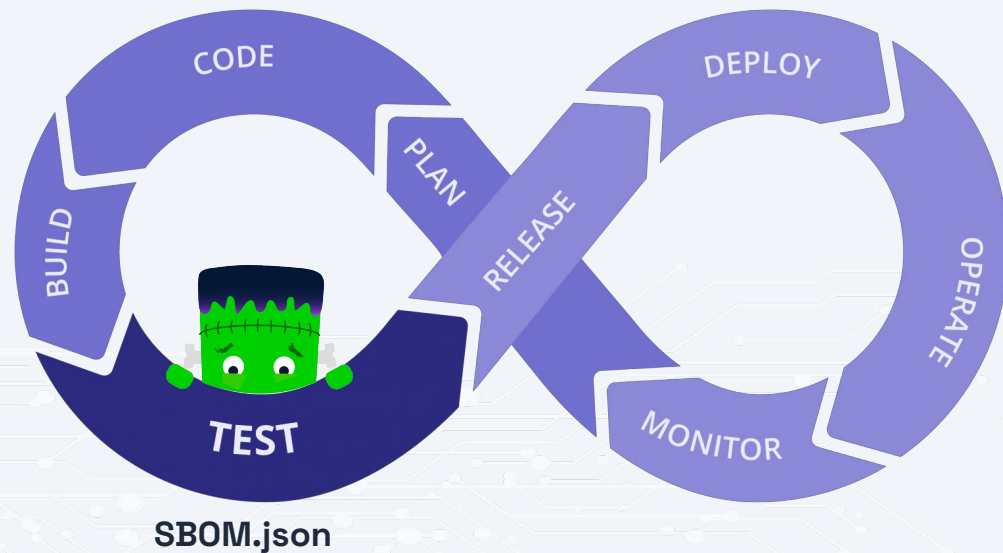
About us

- Disruptive **Technology**
 - Open Source
- Disruptive **Revenue Model**
 - Data Subscription
- **Built for developers: Shift left**



Automate - Everything As Code

- SCA Validation
- SBOM
 - With your code
 - In your revision history
- Precise identifications



License Compliance, Export Control and Security

**“You can’t protect or comply with
what you can’t see”**

A decorative background pattern of white circuit board traces and nodes on a light blue gradient background, extending across the bottom half of the slide.

Detecting undeclared software

Detecting declared software

- Reading software metadata
- Copyright statements
- License files and headers
- Dependency files

Detecting undeclared software

- Files without license headers
- Built-in dependencies
- Stripped headers
- Plagiarism detection
- Critical for embedded systems

Detecting known fingerprints

```

urepath = ''
for basis in ( 'basis-link', 'basis', '' ):
    for ure in ( 'ure-link', 'ure', 'URE', '' ):
        if os.path.isfile(realpath(basepath, basis, ure, 'lib', 'unorc')):
            urepath = realpath(basepath, basis, ure)
            info(3, "Found %s in %s" % ('unorc', realpath(urepath, 'lib')))
            # Break the inner loop...
            break
        # Continue if the inner loop wasn't broken.
        else:
            continue
    # Inner loop was broken, break the outer.
    break

```



Your code fingerprint

```

file=24e35278ad5d4d3babe7379dc34d5bce,439,pasted.wfp
5=369450fc
6=bf7226a9
8=b04dd861
9=9727e3cd
11=2152ba16

```



```

{
  "snippet.py": [
    {
      "id": "snippet",
      "status": "pending",
      "lines": "1-10",
      "oss_lines": "165-174",
      "matched": "90%",
      "purl": [
        "pkg:github/unoconv/unoconv",
        "pkg:deb/unoconv",
        "pkg:pypi/unoconv"
      ],
      "vendor": "unoconv",
      "component": "unoconv",
      "version": "0.8.2",
      "latest": "0.8.2",
      "url": "https://github.com/unoconv/unoconv",
      "release_date": "2017-12-07",
      "file": "unoconv",
      "url_hash": "c36074c3996ba9d7d85f4a57787b5645",
      "file_hash": "0f55e083dcc72a11334eb1a77137e2c4",
      "source_hash": "aff32ef2847f81abc62da0769bfff43f",
      "file_url": "https://osskb.org/api/file_contents/0f55e083dcc72a11334eb1a77137e2c4",
      "licenses": [
        {
          "name": "GPL-2.0-only",
          "obligations": "https://www.osadl.org/fileadmin/checklists/unreflicenses/GPL-2.0-only.txt",
          "copyright": "yes",
          "patent_hints": "yes",
          "incompatible_with": "Apache-1.0, Apache-1.1, Apache-2.0, BSD-4-Clause, BSD-4-Clause-UC, FTL, IJG, OpenSSL, Python-2.0, zlib-acknowledgement, XFree86-1.1",
          "source": "component_declared"
        }
      ]
    }
  ]
}

```

JSON response

Why is SCANOSS better?

- Open Source
 - Safer, no more secret hashing / data handling
 - The end of vendor lock-ins
- Specially designed snippet DB engine
 - Better, Faster, Stronger
- Accurate, complete, actionable SBOM
 - Declared + undeclared, precise IDs
- Inbound SBOMs solved
 - Supply Chain Transparency

Rapidly growing ecosystem

Open Source Tools



OSS Review Toolkit

FOSSLight



fossology

SCA Vendors

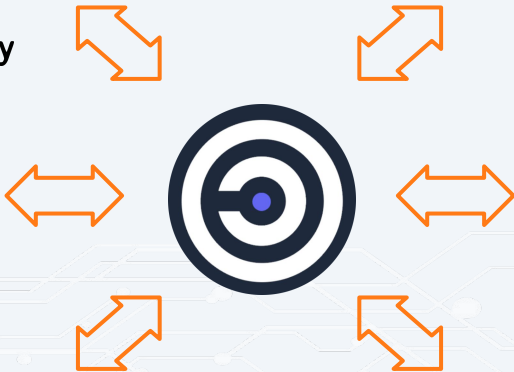
Law firms



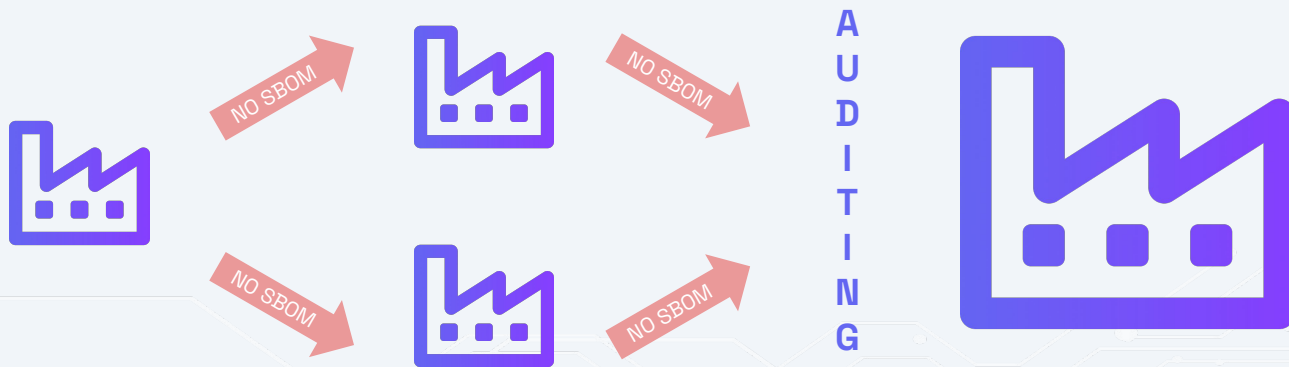
Universities

Audit providers

Supply Chain Requirements



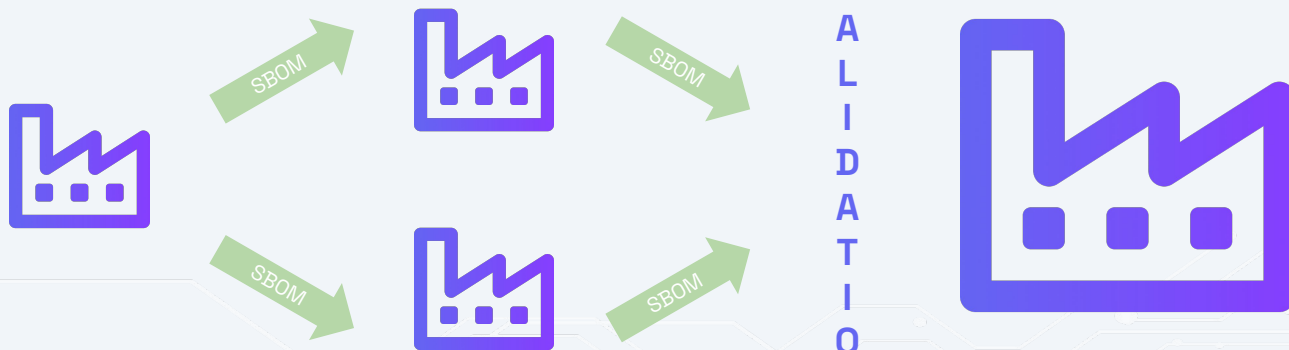
Driving SBOM Adoption



Small and Medium Enterprises

Large Enterprises

Driving SBOM Adoption



Small and Medium Enterprises

Large Enterprises

Presence in public repositories

```
$ pip3 install scanoss  
$ scanoss-py scan mycode/
```

```
$ npm install -g scanoss  
$ scanoss-js scan mycode/
```




<https://github.com/scanoss>

First Multi-platform Auditing App

mycode > Reports Export

Detected Identified

Licenses



- GPL-2.0-only
- BSD-3-Clause
- Apache-2.0
- The Apache Software License: Version 2.0

Matches for license

Component	Vendor	Version
mzmine3	mzmine	Windows-latest

Matches

96% Match

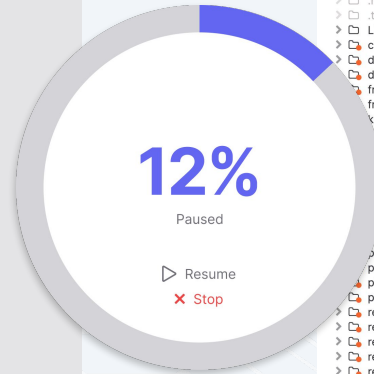
Scanned Files: 1783

4% No Match

Vulnerabilities

0 CRITICAL 0 HIGH 0 MODERATE 0 LOW

LICENSE	COPYLEFT	INCOMPATIBLE LICENSES
GPL-2.0-only	✓	Apache-1.0 Apache-1.1 Apache-2.0 BSD-4-Clause BSD-4-Clause-UC FTL LGPL OpenSSL Python-2.0 zlib-acknowledgement XFree86-1.1
BSD-3-Clause	✗	
Apache-2.0	✗	
The Apache Software License: Version 2.0	✗	
BSD	✗	
MIT	✗	



mycode > Detect

mycode

- github
- reuse
- travis
- LICENSES
- cli-scanner
- docker
- docs
- frontend-apps
- frontend-bugs
- kb-importer
- ubernetes
- g
- g-java
- g-java-init
- g-java-reach
- g-java-reach-soot
- g-java-reach-wala
- g-python
- patch-analyzer
- patch-lib-analyzer
- plugin-gradle
- plugin-maven
- repo-client
- rest-backend
- rest-lib-utils
- rest-lib-utils-init
- rest-nvd
- shared
- dockerignore
- gitattributes
- gitignore

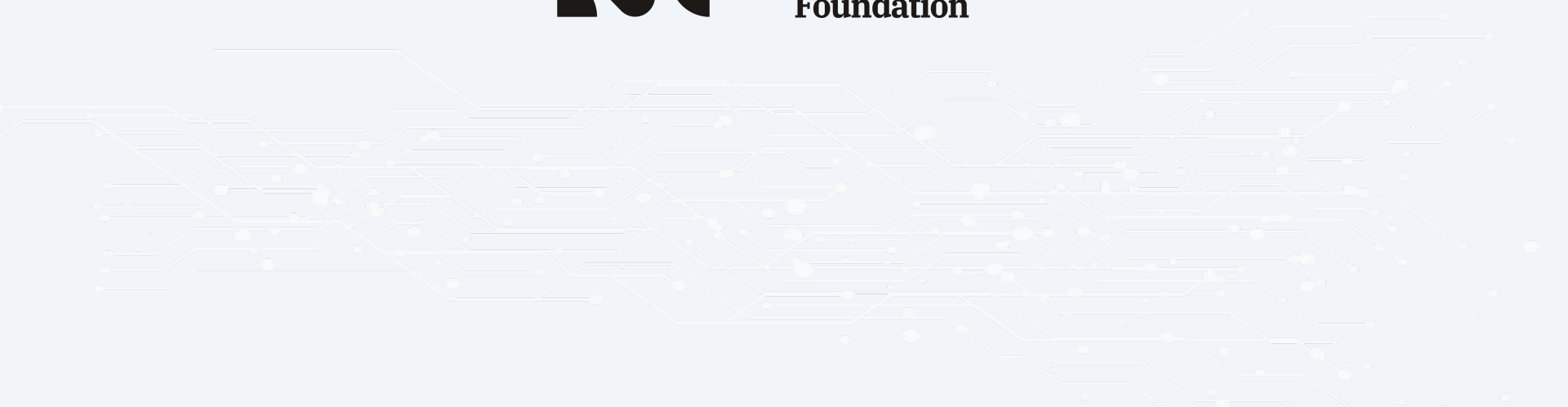
9 versions **steady** 822

24 versions **cxf** 512

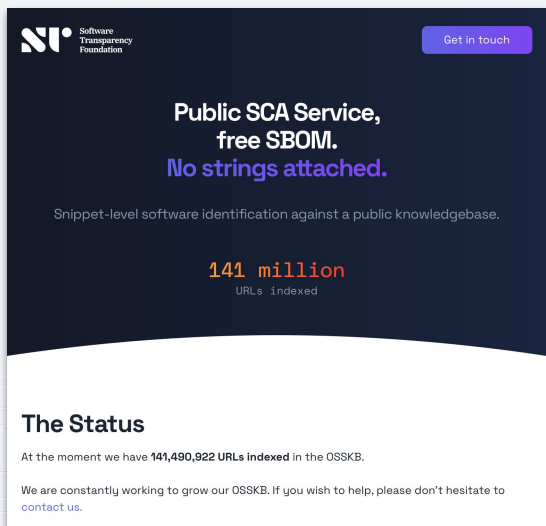
3 versions **cxf-rt-ws-security** 32

5 versions **commons-fileupload** 7





Foundation Projects



Software Transparency Foundation

Get in touch

Public SCA Service,
free SBOM.
No strings attached.

Snippet-level software identification against a public knowledgebase.

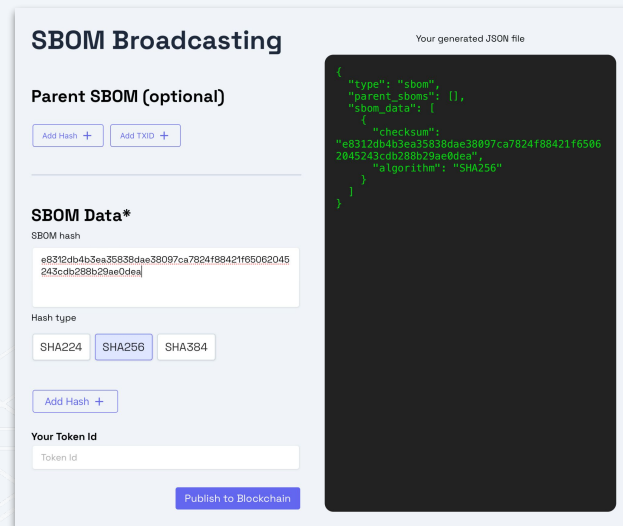
141 million
URLs indexed

The Status

At the moment we have 141,490,922 URLs indexed in the OSSKB.

We are constantly working to grow our OSSKB. If you wish to help, please don't hesitate to [contact us](#).

OSSKB.ORG



SBOM Broadcasting

Parent SBOM (optional)

Add Hash + Add TXID +

SBOM Data*

SBOM hash

e8312db4b35ea35838dae38097ca7824f88421f65062045243c9b288b28ae0dea

Hash type

SHA224 SHA256 SHA384

Add Hash +

Your Token Id

Token Id

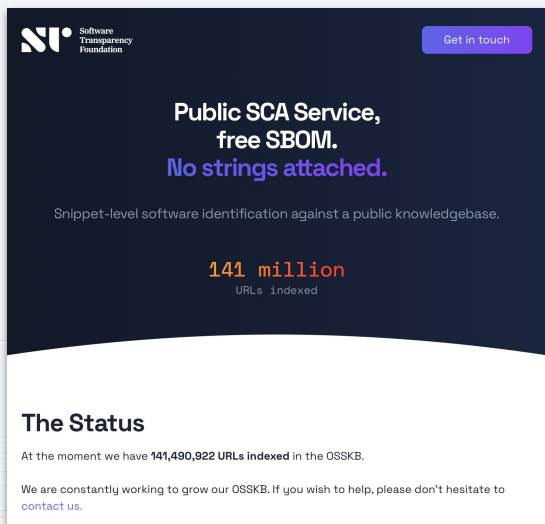
Publish to Blockchain

Your generated JSON file

```
{
  "type": "sbom",
  "parent_sboms": [],
  "sbom_data": {
    "checksum":
      "e8312db4b35ea35838dae38097ca7824f88421f6506
      2045243c9b288b28ae0dea",
    "algorithm": "SHA256"
  }
}
```

SBOM.INFO

Public API Service



The screenshot shows the OSSKB website with a dark blue header and a white footer. The header contains the STI Software Transparency Foundation logo and a 'Get in touch' button. The main content area is dark blue with white and purple text. The footer is white with black text.

STI Software Transparency Foundation [Get in touch](#)

**Public SCA Service,
free SBOM.
No strings attached.**

Snippet-level software identification against a public knowledgebase.

141 million
URLs indexed

The Status

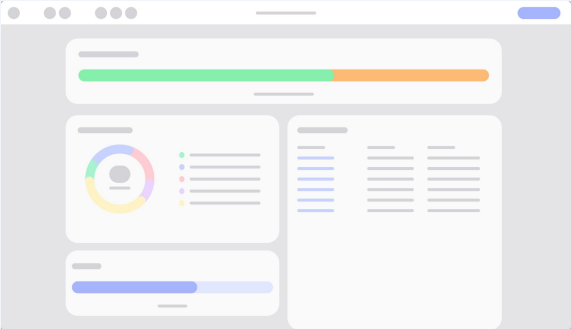

At the moment we have **141,490,922** URLs indexed in the OSSKB.

We are constantly working to grow our OSSKB. If you wish to help, please don't hesitate to [contact us](#).

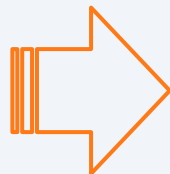
- Free of charge
- Perpetual
- Safe
- Anonymous
- Stateless

OSSKB.ORG

Public Knowledge Base API



```
$ scanoss-py scan  
$ scanoss-js scan
```



<https://osskb.org/api>

Available offerings



Knowledgebase Updates	Quarterly	Monthly (On-prem) / Daily (SaaS)
Layers of information	<ul style="list-style-type: none"> • SBOM generation • Snippet detection • Licenses • PURL array 	<ul style="list-style-type: none"> • SBOM generation • Snippet detection • Licenses • PURL array • Copyright statements • Attribution notices • CPE • Vulnerabilities • Dependencies • Cryptography • Quality • Health • Security
Availability + throughput	<ul style="list-style-type: none"> • Best Effort • University Mirrors 	<ul style="list-style-type: none"> • Guaranteed
Audit Workbench	<ul style="list-style-type: none"> • Standalone 	<ul style="list-style-type: none"> • Enterprise • SAML/SSO • Shared workspaces
Support	<ul style="list-style-type: none"> • Community 	<ul style="list-style-type: none"> • Dedicated + SLA • Custom integrations



Thank you!

Julian Coccia - CTO

<https://scanoss.com>