



# osskb.org

How to create a complete SBOM using  
open source tools

# Table of Content

1. Speakers
2. Introduction
3. About osskb.org: overview
4. Demo 1: detection
5. About osskb.org: technical description
6. Demo 2: enrichment
7. About STF: overview
8. Demo 3: SBOM
9. About STF: other details
10. Demo 4: workflow
11. Summary



# Speakers



## Agustín Benito Bethencourt

- STF Ecosystem Lead. [Consultant](#). [Bio](#).
- About osskb.org and STF

## Matias Daloia

- Software Engineer @ SCANOSS. [LinkedIn](#)
- Demos: osskb.org and workflows

## Óscar Enrique Goñi

- Core SW Engineer @ STF/SCANOSS. [Linkedin](#)
- Demo: FOSSology integrated with osskb.org

## Agustín Isasmendi

- Software Engineer @ SCANOSS. [LinkedIn](#)
- Demo: Snippets Detection with ORT

## Jerónimo Ortiz

- DevSecOps @ SCANOSS. [LinkedIn](#).
- Demos: Detection. SBOM.



# Introduction



You can't protect or comply with what you  
cannot see

.-SCANOSS dixit



# Create a complete, standardised and up-to-date SBOM of our software composition

1. Know all the SW components within your software composition
  - **Detect** all the **open source** components/snippets
  - Identify them: curation
2. **Enrich** the information with additional metadata associated to each one of those components, depending on the SBOM purpose/type
3. Express (declare) the enriched information in a standardized taxonomy
  - CycloneDX
  - SPDX



This talk aims to demonstrate...

.... the benefits of using **osskb.org** ...

... with existing open source SCA tools ...

... to create complete, standardized and up-to-date SBOMs ...

... in a modern way





# About [osskb.org](https://osskb.org)



# osskb.org overview

osskb.org:

- Is a [Software Transparency Foundation](#) service
- Provides universal and free of charge access to **OSS Knowledge Base (KB)**
- Is accessible through an open API ([scanoss-api\[1\]\[2\]](#)).
- Is designed as a back-end data-based service for:
  - Open source SCA tooling (scanners, auditing, analyzers, SBOM generators...) developers
  - Platform engineers: pipelines integration (at limited scale)
  - Upstream developers, Open Source projects, R&D projects
  - Auditors, IP and license compliance experts

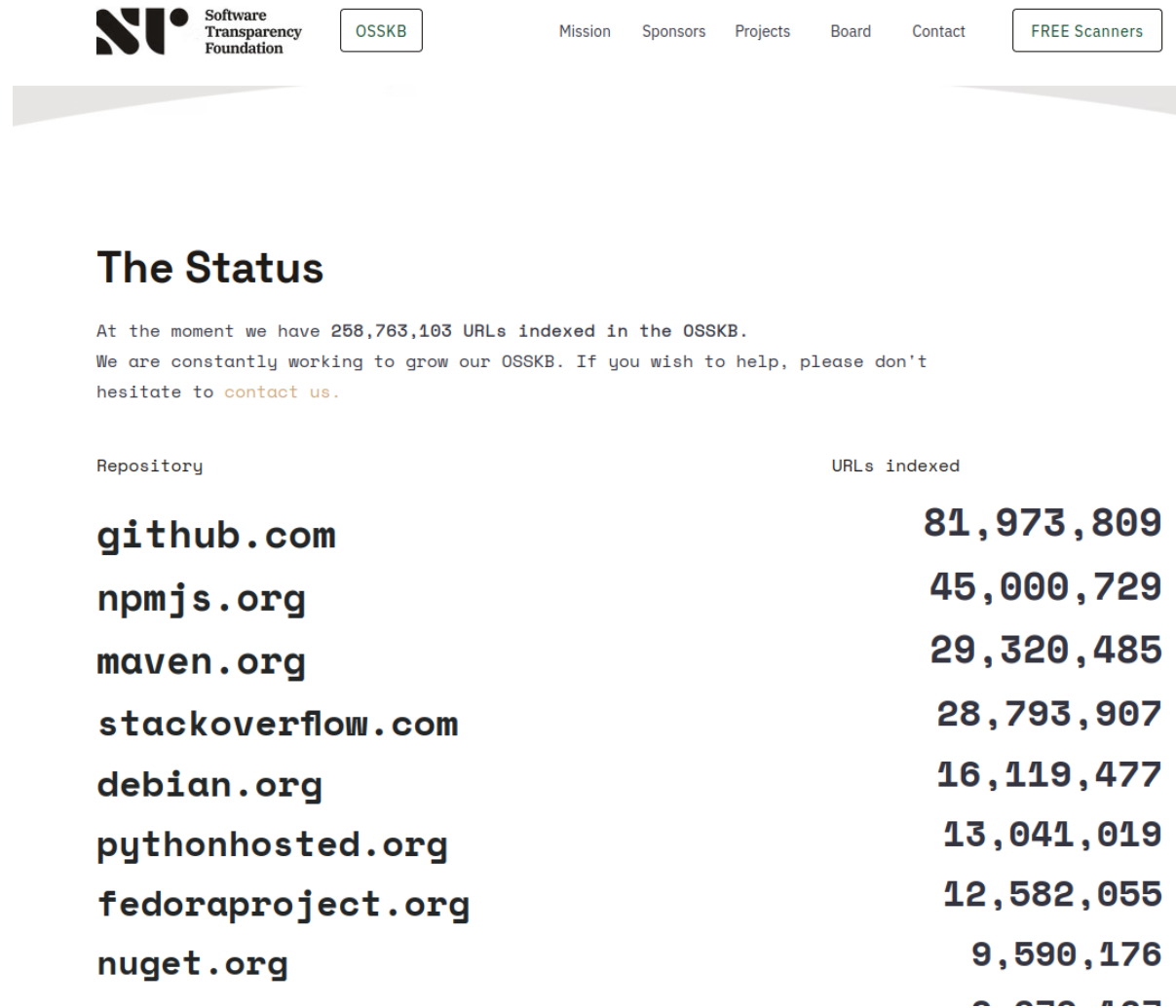


- Growing service: ~200k scanned files per month a year ago, today ~1M
- STF guarantees a minimum QoS for all through several actions:
  - There are calls/scanned-files per month limits
    - Currently, around 30k files/month
    - This amount is increasing over time thanks to Members (specially SCANOSS)
  - STF detects and manages potential outliers
  - STF Members get higher levels of QoS (higher limits)
  - Specific usage agreements for special cases are possible

# OSS KB

- osskb.org is powered by [OSS KB](#)
- OSS KB is not a DDBB but a hash-based data structure, including ...
  - Hashes, matching *all* published open source software.
  - An open source intelligence layer: licenses and copyright statements
  - Advanced detection capabilities, at file and snippet level

[ABOUT osskb.org](#)



The screenshot shows the OSS KB website header with the Software Transparency Foundation logo, a navigation menu (Mission, Sponsors, Projects, Board, Contact), and a 'FREE Scanners' button. Below the header is a section titled 'The Status' with a paragraph of text and a table of repository statistics.

At the moment we have 258,763,103 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](#).

Repository	URLs indexed
<a href="#">github.com</a>	81,973,809
<a href="#">npmjs.org</a>	45,000,729
<a href="#">maven.org</a>	29,320,485
<a href="#">stackoverflow.com</a>	28,793,907
<a href="#">debian.org</a>	16,119,477
<a href="#">pythonhosted.org</a>	13,041,019
<a href="#">fedoraproject.org</a>	12,582,055
<a href="#">nuget.org</a>	9,590,176



With OSS KB you can...

1. Detect **declared and undeclared** OSS in your SW composition so you can:
  - a. Create a complete SBOM
  - b. Audit third party software
2. Check **against plagiarism** of any OSS introduced ...
  - a. By copy/paste or by AI-assistants
  - b. Across your supply chain
  - c. At build time, through dependencies
3. Apply open source intelligence across your workflow:
  - a. Development process: integration with IDEs, pre-commit hooks ...
  - b. Delivery processes: integration with pipelines at different stages ...
4. Prototype some complex set-ups, policy checks, further integrations, transparent audits across supply chains ...



- OSS KB was created, and it's maintained by [SCANOSS](#) for STF.
- SCANOSS provided to the [STF](#) a perpetual license to host and provide universal, free of charge (gratis) access to OSS KB
- Two key concepts related with OSS KB (differentiators):
  - Privacy by design
  - No vendor lock-in



# Demo 1: detection



## Demo 1: detection using osskb.org

- Goal:
  - Open Source detection: declared and undeclared **components**
  - Open Source detection: declared and undeclared **dependencies**
- Tools tech. and services:
  - [scanoss.py](#). [User guide](#). License: MIT
  - [osskb.org](#) from [STF](#) as back-end
- Example components:
  - zlib 1.3.1. Chosen for showing osskb capabilities, especially, when detecting C language dependencies





# More about [osskb.org](https://osskb.org)



## More about osskb.org

- Any open source SCA tool can use osskb.org as back-end ...
  - ... by implementing the openAPI
- Open Source tools integrated with osskb.org
  - SCANOSS scanners, auditors and analyzers
  - FOSSology
  - FOSSlight
  - ORT
  - Theia IDE (announced yesterday)
- osskb.org operations built/run with open source: Docker, Ansible, pip...
- OpenAPI and Open Source SCA clients guarantee transparency using osskb.org



## More about OSS KB

- OSS KB is created, updated, integrated, operated... **using OSS** (do not reinvent the wheel!):
  - Open Source intelligence : Scancode, Semgrep, algorithms implementations...
  - The KB itself (dogfooding): Minr, ldb...
- No vendor lock-in
  - The KB technology behind OSS KB is also open source
- Create your own KB, then...
  - ... build your own service for your own users or/and ...
  - ... make your own KB globally available through [osskb.org](https://osskb.org)



OSS KB offers privacy by design...

- Hashes created using [an open source implementation](#) of the winnowing algorithm.
- Hash-based comparison vs file/component comparison
  - STF/SCANOSS does not know what are you scanning
- Scanners scan against OSS KB (through [osskb.org](https://osskb.org)), not the other way around
- No identification required to use [osskb.org](https://osskb.org) (anonymity)



# Demo 2: enrichment



## Demo 2: enrichment and snippet detection

- Goals:
  - Enrichment: licenses and copyright statements
  - Detection: snippets
- Tools tech. and services:
  - [FOSSology](#). [User guide](#). License: GPL 2.0 and LGPL 2.1
  - [ORT](#). [User guide](#). License: Apache-2.0
  - [osskb.org](#) from [STF](#) as back-end.



# About STF: overview



## About STF

- *Fundación para la Transparencia del Software* ([STF](#)) IS a foundation
- Registered in 2021 in Madrid, Spain. EU
- The STF operates under the following **principles**:
  - Openness
  - Transparency
  - Open Collaboration
  - Open Governance
  - Vendor neutrality





# STF's mission

STF's **Mission**: "Bring transparency to the software supply-chain"

1. Driving adoption of SBOMs → [osskb.org](https://osskb.org)
2. Enabling a decentralised validating entity → [SBOM Ledger](#)
3. Facilitating SBOM interoperability



# STF governing bodies

## Board of Trustees:

- Main governance body of the STF according to Spanish Law of Foundations.
- Legal representation of STF
- Monitors that STF Principles, Mission and good governance practices are followed
- Ratifies the main Governing Board decisions: budget, reports, Charter...
- President: José María Lancho Rodríguez [1]



## Governing Board Role:

- Management of the STF as organization and oversee of all the activities
- Steers STF activity towards meeting the key objectives
- New Members and projects approval
- Create and approve the [Charter](#) and [Participation Agreement](#)
  - Current ones were approved on 2024-11-15

## Governing Board Members:

- [Representatives](#) from the different Governing Bodies
- Strategic, Gold, Silver (organizations), and Community (orgs., projects or individuals)
  - Strategic Members, so far: SCANOSS and Huawei



# Demo 3: SBOM



## Demo 3: SBOM generation and update

- Goals:
  - SBOM generation in SPDX and Cyclone DX
  - SBOM update
- Tools tech. and services:
  - [scanoss.py](#). [User guide](#). License: MIT
  - [osskb.org](#) from [STF](#) as back-end.



# More about STF



# Key Actions 2025

- Increase awareness about STF and osskb.org
- Incorporate new Members to STF
- Increase osskb.org capacity
- Development and data projects governance processes
- Host open data sets, donated by SCANOSS:
  - [Purl2cpe](#)
  - [Crypto algorithms open dataset](#)
    - Starting point of the coming SPDX crypto algorithms list
- Support research activities: check the [first paper](#) of 2025



## Collaborate with STF by ...

- Using osskb.org
- Promoting osskb.org among the open source projects which software you consume
- Becoming an STF Members, helping STF to scale up osskb.org
- Integrating osskb.org with your SCA tool or IDE of choice, your workflow...
- Creating your own KB and making it universally available through osskb.org
  - Becoming the origin and *source of truth* for your software across any supply chain





# STF resources

- STF Website: <https://www.softwaretransparency.org/>
  - Approved Governing Board [meeting minutes](#)
  - [Charter and Participation Agreement](#)
- Contact [form](#)
- STF mailing list: <https://www.freelists.org/list/st-foundation>
- STF in social media: LinkedIn [page](#)



# Demo 4: workflows



## Demo 4: ... in a modern way: workflow integrations

- Goals:
  - osskb.org as part of the development workflow
  - osskb.org as part of the delivery workflow
- Tools tech. and services:
  - Pre-Commit hooks. [Repository](#). License: MIT
  - Scanoss Code Compare [Repository](#). License: MIT
  - GitHub Action integration [Repository](#). License: MIT
  - [osskb.org](#) from [STF](#) as back-end.



# Summary



- STF and OSPOs share a common purpose: upstream projects distribute complete, standardized and up-to-date SBOMs as part of their software releases
  - So OSPOs can audit them and incorporate them to their bill of materials
- osskb.org tackles one of the most fragile steps to achieve that purpose: detecting open source at both, the file and snippet levels
  - Osskb.org helps in several other steps
- osskb.org was designed:
  - With a data mind set vs the classical application mind set
  - Flexibility by design: serves various purposes, compatible with any tooling, adaptable to different workflows
  - ...
  - Privacy by design. No vendor lock-in
- STF is the organization providing osskb.org under transparent conditions and values



Thank you:

- To the OSPO Alliance for the invitation
- To SCANOSS engineers for the demos

Questions?



# osskb.org

How to create a complete SBOM using  
open source tools