SCANOSS

SCA With Open Source Tools and Technologies

OpenChain Tooling Group

Tooling Group weekly meeting
2025-02-19

Jeronimo Ortiz
DevSecOps Engineer

Table of Content

About SCANOSS and Software Transparency Foundation

SCANOSS: the company

- Software Composition Analysis (SCA) disruptor
- Registered in Madrid, Spain, EU. Remote-only company +30 staff (2024Q4)
- SCANOSS is a **data company**, being SCANOSS KB our IP
- Target market: open source software intelligence at scale (big corporations)
- Committed to open source:
  - 100% free and open source software developed in the open
  - Privacy by design: strong differentiation factor
  - Zero vendor lock-in: create your own knowledge base with SCANOSS tech
  - Participation in several open source projects and vendor neutral forums. STF founding members
  - Two open data sets (CC0) published[1][2]. Stay tuned for more!

Software Transparency Foundation, osskb.org and OSSKB

- STF (Madrid, Spain. EU.) has as mission "Solving Software Supply Chain Transparency"
- osskb.org is a free of charge service that enables open source upstream devs and projects to create complete SBOMs through SCANOSS and/or third party tools
- osskb.org provides access to OSS KB through an open API (scanoss-api[1][2]).
- OSS KB and SCANOSS KB share:
  - Raw data and scanning capabilities:
    - File and snippet level scanning
    - Detect declared and undeclared OSS in your software
  - Licenses dataset provides actionable intelligence about:
    - License obligations, compatibility, copyright notices, attributions…
    - Support for every language

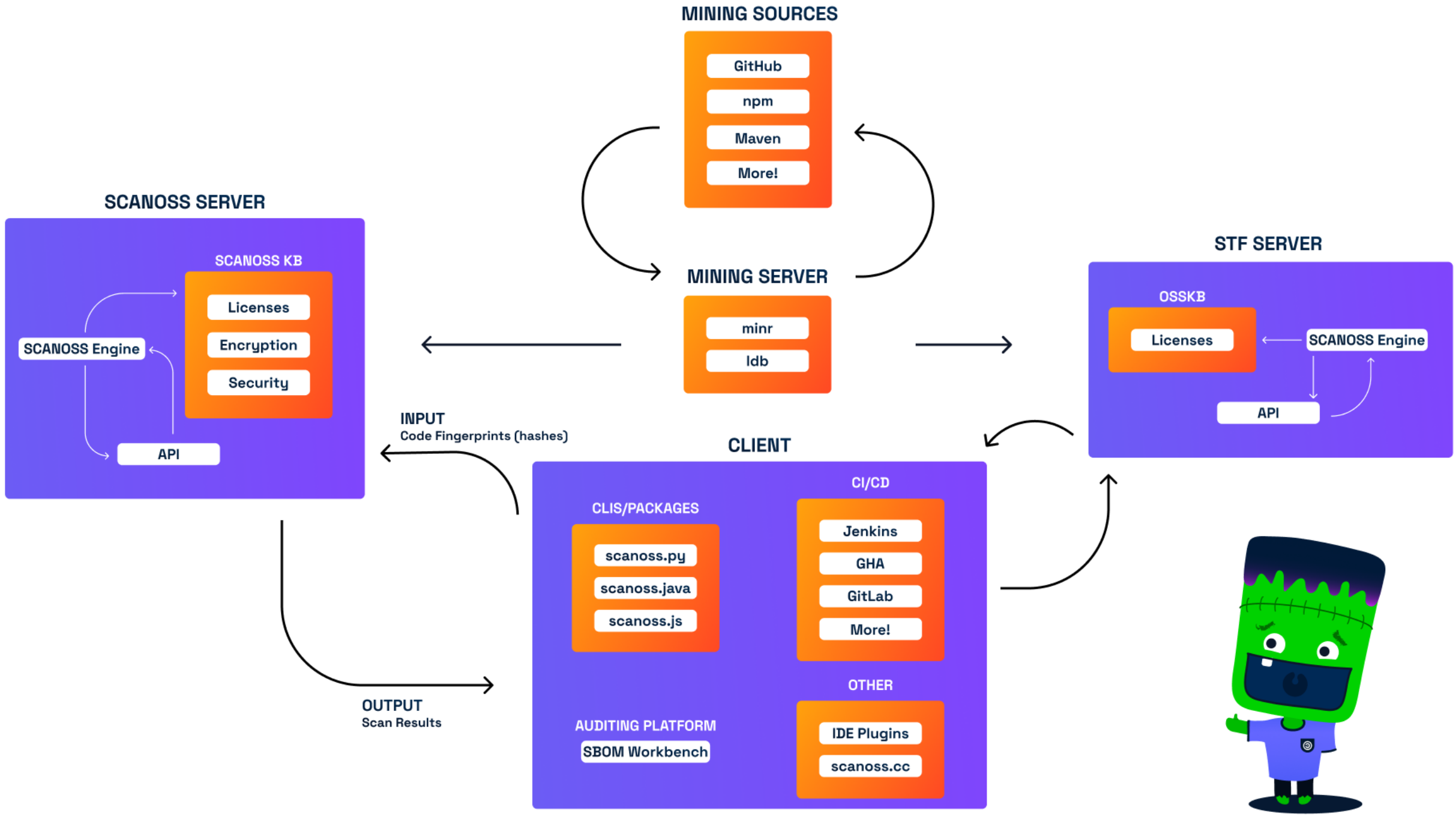
SCANOSS Open Source SCA tools and technologies

Overview

- **Development in the open**
  - Open Source tools and technologies developed on public GitHub repos.
- **Zero vendor lock-in**
  - Build your own KB with SCANOSS technologies
  - Use SCANOSS or third party clients/scanners and openAPIs to use your own KB
- **Privacy by design**
  - Users scan against OSS KB, not the other way around. Hash-based matching
  - No STF account or any other identification required to use osskb.org
- **Extreme flexibility**
  - Seamlessly connect to osskb.org through an openAPI and leverage OSS KB features
  - Scan against osskb.org locally or as part as your CI/CD using open source software

SCANOSS software

Software	Target	Features	License
Minr	Data/Developers	Mine any software. Make your own KB, together with ldb, and test it (test-kb)	GPL-2.0-only
Engine	Developers/DevOps	Deploy and scan against your KB	
API	Developers/DevOps	OpenAPI/Protobuf	
ldb	Developers	DB Management System	
SDK	Developers	Interact with the API, Java SDK.	MIT
CLIs (Python, Java)	Developers	Extract fingerprints, scan against KB and generate SBOMs	
SBOM Workbench	Auditors/Compliance Experts	Audit your software and generate SBOMs	GPL-2.0-only
CI/CD Integrations	DevOps	Jenkins, SonarQube, GitLab and more	
Extensions	Developers	IDE Plugin, scanoss.cc	


MINING SOURCES
GitHub
npm
Maven
More!
MINING SERVER
minr
ldb
SCANOSS SERVER
SCANOSS KB
Licenses
Encryption
Security
SCANOSS Engine
API
STF SERVER
OSSKB
Licenses
SCANOSS Engine
API
INPUT
Code Fingerprints (hashes)
CLIENT
CLIS/PACKAGES
scanoss.py
scanoss.java
scanoss.js
CI/CD
Jenkins
GHA
GitLab
More!
OTHER
IDE Plugins
scanoss.cc
AUDITING PLATFORM
SBOM Workbench
OUTPUT
Scan Results

Demo time!

DEMO TIME!

Detect declared and undeclared OSS. Generate an SBOM

- **Use case:**
  - Scan your source code for declared and undeclared OSS components as well as dependencies and generate an SPDX-Lite SBOM
- **Tools/services used during this demo:**
  - osskb.org
  - scanoss-py
- **Structure:**
  - Set up and overview of the tool
  - Demonstration

DEMO TIME!

Detecting OSS at scale, integrated in your pipelines

- **Use case:**
  - Automatically detect and block pull requests containing undeclared dependencies or copyleft-licensed code to protect the project's licensing compliance on GitHub
- **Tools/services used during this demo:**
  - osskb.org
  - SCANOSS Code Scan Action (GitHub Actions)
- **Structure:**
  - Set up and configuration options
  - Demonstration

Q&A

Resources

SCANOSS

- Web: https://scanoss.com/
- Software/tools: https://github.com/scanoss
- Technical Documentation: https://docs.scanoss.com/

STF

- Web: https://www.softwaretransparency.org/
- osskb.org: https://osskb.org/