FOSSID

Open Source Audits

FOSSID's open source audit services help you understand which open source components that reside in the audited software code base, and if it is compliant with the discovered license requirements.

Due to security and privacy concerns surrounding M&A transactions, FOSSID has designed and implemented the unique ability to perform audits and generate reports without looking at the target source code. This is referred to as a "blind audit".

FOSSID Blind Audits

The output of an audit service includes several comprehensive reports, giving you full insight into which open source components, files and snippets that reside in the audited code base, together with their origins and licenses.

Open Source Inventory or Bill of Materials (BoM)

The BoM report lists all detected 3rd party open source components, files, and code snippets. Its interactive capabilities facilitate the filtering and reviewing of the audit findings, and the creation of follow-up actions.

Security Vulnerabilities Report (CPE-CVE)

This report lists all detected security vulnerabilities and exposures (CVEs) and corresponding Common Platform Enumerations (CPEs) according to the National Vulnerability Database (NVD) and other sources.

Software Package Data Exchange® (SPDX)

SPDX® is an industry standard format for communicating the components, licenses and copyrights associated with software packages. This report is essentially a software inventory XML file that can be imported into other tools.

Executive Summary

The executive summary summarizes the findings and observations from the other reports, giving the reader a high-level understanding of the overall open source licensing and security vulnerability status of the audited software.

@fossid_ab
linkedin.com/company/fossid-ab/

www.fossid.com

FOSSID Blind Audits

Initial Meeting

A first conference call takes place to kick start the project, introduce contact persons from all parties and communicate relevant details of the audit such as timeline, custom reports, etc.

Fingerprint Collector Tool

FOSSID's Command Line Interface (CLI) is provided to the target company along with installation and execution instructions to collect digital signatures (fingerprints) of their software.

Collection of Digital Signatures

The collection of digital signatures cannot be reverse engineered to the original source code, but is enough for FOSSID to perform the audit.

Secure Transfer

The collection of digital signatures is transferred securely over SSH to a dedicated server in FOSSID's datacenter.

Knowledge Base Comparison

The collection of digital signatures is used to search the biggest open source database in the industry and find matches to open source files and snippets.

Blind Audit

FOSSID compliance engineers audit the target software without having access to the actual source code.

Approval Request

Once the audit is concluded, all reports are sent to the target company for approval before they are shared with the potential buyer.

Report Delivery

After the approval, the final reports are transferred securely to the potential buyer, including the Bill of Materials, SPDX, executive summary and more.

Final Meeting

Another conference call takes place to present the audit results and answer any question that might have arisen from the reports.

FOSSID offers a state-of-the-art open source scanner that integrates in your development process seamlessly and detects pieces of Free and Open Source Software (FOSS) in your code base, from entire components to code snippets. FOSSID's software uncovers license obligations and compliance issues so that you can focus on creating great products.

@fossid_ab
linkedin.com/company/fossid-ab/

www.fossid.com

GET IN TOUCH

Discover all FOSSID products and services at www.fossid.com

This datasheet is for informational purposes only. FOSSID makes no warranties, express or implied, with respect to the information presented here.

FOSSID AB
Gåsgränd 3
111 27 Stockholm
Sweden

FOSSID K.K.
1-10-3-200 Roppongi, Minato-ku
Tokyo 106-0032
Japan