Metrics To Evaluate Source Code Scanning Tools

There are a number of existing open source compliance tools in the market. How to decide which one is best for you? Here are a number of metrics that you can refer to when evaluating such tools.

- ***Size of the knowledge base*** against which scanned code is being compared
- ***Frequency of updates to the knowledge base* -** how often does the tool provider update the knowledge base to keep up with the pace of open source development?
- ***Speed of scans*** for the same loads
- ***Supported deployment models* -** cloud, on premise, hybrid
- ***Ability to identify origin and license of snippets*** - many tools do not provide such support and are only capable of identifying whole open source components, others have poor support
- ***Ability to auto-identify open source snippets*** in scanned code flagging their component of origin and license - saving endless hours on manual labor
- ***Support for vulnerability discovery*** - is the tool capable of identifying vulnerable code that was copy/pasted from one component into another? Or simply just able to identify vulnerabilities found in their original components
- ***Ability to represent and manage end-to-end review and approval process*** directly from within the tool via a self defined workflow
- ***Total cost of ownership*** - *which include the yearly license cost, training cost, cost of customizations (workflow, features, integration, etc.), cost of servers required for your specific install and Internal sys admin support for your install*
- ***An intuitive UI* -** easy and inviting to use – minimizing learning curve and making it less of a chore
- ***Support for APIs and a CLI*** that you can interconnect with your CD/CI environment to for ease of integration with existing development and build systems
- ***Ability to use the tool for M&A transactions*** without restrictions on the use of the tool as part of the licensing agreement
- ***Support for different audit methods*** - several methods exist
- ***Programming languages agnostic*** - the tool should be able to process any source code regardless of the programming language
- ***Support for SPDX*** - discovering licenses declared using SPDX identifiers and exporting scan results in SPDX format
- ***Ability to represent company policies and apply them on scanned code*** triggering specific actions depending on the license of the scanned code and related policies

Read more on practical open source compliance: Download free ebook "Open Source Compliance for the Enterprise" (2nd Edition).

Original Author:
Ibrahim Haddad