Tools: Source Code Scanning and License Compliance

Return to Tools Area

Source: Tools for managing open source programs

- ***Antepedia Reporter*** *– A commercial, fee-based application from Antepedia, Reporter is a report-generation product which lets developers, project managers, legal advisors and others create license compliance audits and Intellectual Property (IP) rights management reports about the open source, public and private components in your code base.*
  http://www.antepedia.com/pages/tools.html
- ***Black Duck Hub*** *– The commercial Hub service scans code to identify all embedded open source components, and then automatically searches for known vulnerabilities for remediation. It can send alerts when new vulnerabilities are found in your code.*
  https://www.blackducksoftware.com/products/hub
- ***Black Duck Protex*** *– Protex is a commercial, fee-based license compliance management tool from Black Duck which integrates with existing tools to automatically scan, identify and inventory open source software, while also enforcing license compliance and corporate policy requirements.https://www.blackducksoftware.com/products/protex*
- ***Copyright review tools*** *– This collection of open source command-line tools help make initial copyright file construction and subsequent review and update easier.*
  https://wiki.debian.org/CopyrightReviewTools
- ***dep-checker*** *– A free dependency checker tool from The Linux Foundation, dep-checker performs a complete analysis of linkages between code packages.*
  http://git.linuxfoundation.org/dep-checker.git/
- ***FlexNet Code Insight*** *– Flexera, which acquired licensing compliance vendor Palamida in 2016, commercially offers Flex Code Insight to help automate corporate open source use among developers, legal teams and security staffers.*
  https://www.flexerasoftware.com/enterprise/products/software-vulnerability-management/flexnet-code-insight/
- ***FOSSA*** *– This is a commercial tool that automatically performs code dependency tracking, license compliance scanning in the background. http://fossa.io/*
- ***FOSSology*** *– A Linux Foundation project, FOSSology is an open-source license compliance software toolkit that can run license, copyright and export control scans from the command line. A database and web UI are also available to create compliance workflows. https://www.fossology.org/*
- ***janitor.git*** *– Code Janitor is an open-source tool that helps evaluate source code for compliance with open source licenses. From The Linux Foundation, Code Janitor can be used with other products to check code. http://git.linuxfoundation.org/janitor.git/*

- ***LicenseFinder*** *– An open-source tool that detects the licenses of the code being used in your projects, compares those licenses against a user-defined whitelist and then provides an actionable report. https://github.com/pivotal/LicenseFinder*
- ***Protecode Enterprise Analyzer*** *– This commercial application is used to analyze and identify all code in any directory to determine code ownership and ensure open source license compliance based on predetermined internal policies. http://www.protecode.com/our-products/system-4/enterprise-analyzer/*
- ***scancode-toolkit*** *– From nexB, the open source ScanCode suite of utilities scans code for licenses, copyright, and dependencies to find, discover and inventory open source and third-party components used in your code. https://github.com/nexB/scancode-toolkit*
- ***SPDX*** *– The Software Package Data Exchange (SPDX) specification is a standard format used to describe the components, licenses, and copyrights associated with software packages. The SPDX standard aids compliance with free and open-source software licenses by standardizing the way license information is shared between developers and companies. The SPDX specification is developed by the SPDX workgroup, which is hosted by The Linux Foundation. The group offers open-source tools to help users of SPDX documents. https://spdx.org/tools*
- ***WhiteSource*** *– Provides licensing, security, code quality, and reporting analysis for managing open source components in real-time by automatically and continuously scanning dozens of open source repositories on a commercial basis. https://www.whitesourcesoftware.com/*