Open Source Software Management

Critical Data and Functionality for Managing Security, Obsolescence, and Licensing Risk associated with Open Source Software

August 2023

Minimizing the Risks of Utilizing Open Source Code

According to Github's "Octoverse 2022: The State of Open Source Software" Report, 97% of proprietary and commercial software applications utilize some amount of open source code, and 90% of companies use open source in some manner. Relying on open source to this extent requires a large degree of trust in the quality of the code, as well as some acceptance of potential risks presented by vulnerabilities, obsolescence, and licensing.

The best way to counter these risks is to minimize the unknown:

- What open source code is included in an application?
- What components and libraries are part of that code?
- Are there any known vulnerabilities that put your IT and business operations at risk?
- Have any of the libraries or components that you are utilizing been rendered obsolete by newer versions?
- Are you leveraging Permissive open source license types or more restrictive ones that expose your organization to legal and financial risk?

Eracent's solutions can help you answer these questions for every application in your environment.

Reducing Security Risks through Vulnerability Management and SBOM Analysis

Eracent maintains and curates the IT-Pedia® Open Source Library, which provides essential – and up to date – information about potential vulnerabilities within open source components and libraries. This vulnerability data is a foundational piece for any cybersecurity program.

This data is critical input for Eracent's ICSP Application Risk Management (ARM) module. The ARM module provides a consolidated repository, comprehensive management, and automated analysis for every SBOM (Software Bill of Materials) that an organization has for the applications that it utilizes. In conjunction with Eracent's ITMC Discovery™, the Application Risk Management module provides a match between known vulnerabilities and any installed software that may contain potentially vulnerable open source components and libraries.

Supporting Obsolescence Management

It's important to know whether the applications that you are running are up-to-date or far behind in regard to the components and libraries that they contain. Older code is more likely to be neglected and at a higher risk of containing vulnerabilities. Many times, Application Security and Development (AppSecDev) teams are not aware that a newer version of an open source component or library is available, so they do not perform upgrades. The IT-Pedia Open Source Library and Application Risk Management module provide a listing of all versions of a package, an indicator of which version is the most current, and the Release Date and End of Life and/or End of Support Dates for each one. This information enables you to know precisely how current your code base is.

Minimizing Open Source Licensing Risks

It's crucial to be aware of the open source license categories that are being used within your applications, whether they are commercial or homegrown/proprietary/bespoke. Using code with Permissive licensing is always a safe bet, while CopyLeft and other more restrictive license types can expose your organization to legal and financial ramifications. You can protect your organization's IP and avoid financial penalties by being aware of open source licensing before you incorporate components and libraries into your code base. The IT-Pedia Open Source Library and Application Risk Management module provide this level of detail for each component and library.

The IT-Pedia® Open Source Library

The IT-Pedia Open Source Library underpins all of Eracent's open source management functionality. This invaluable resource provides a highly curated, constantly updated library that puts details about your open source code at your fingertips. There's no need to perform lengthy manual searches across multiple open source repositories to get the information that you need.

Features

The IT-Pedia Open Source Library includes many critical data points:

- The name of the Repository in which each open source product is tracked, demonstrating that an authoritative, trusted source has been referenced
- Group Name
- Package Name
- Version
    - Includes a notation if it is the latest available version
    - Shows if a subsequent version of a library changes from one URL to another in a repository
- PURL
- License
- License Category
- Vulnerabilities
- Lifecycle Data, including:
    - Start of Life
    - Release Date
    - End of Support
    - End of Life

Users can create, add, name and save filters to optimize the efficiency of their searches.

The Open Source "My Products" View

As with the parent IT-Pedia® IT Product Data Library, the IT-Pedia Open Source Library includes a "My Products" view in the user interface. This enables you to streamline your interface and reduce noise by managing only the open source components and libraries that your organization is currently utilizing. Of course, you may add new ones at any time.

Who can benefit from using Eracent's Open Source Management Solutions?

- Cybersecurity, Risk Management and Network Security programs
- Software Asset Management (SAM) programs
- Application Security and Development Teams for software providers and internal development teams.

For more information about the ICSP Application Risk Management Module, the IT-Pedia Open Source Library, or any of Eracent's other solutions for IT Visibility and Foundational Data, Software License and Entitlement Management, and IT Cyber and Risk Management, contact us at info@eracent.com or visit www.eracent.com.

Eracent, Inc.
519 Easton Road, P.O. Box 647
Riegelsville, PA 18077 USA

info@eracent.com
+1- 908-537-6520

www.eracent.com