



# **SBOM Manager <sup>TM</sup>**

*Comprehensive SBOM Management and Analysis:*

*A Critical Component for Ensuring Software Supply Chain Security*

## **SBOM Manager™**

### *A Critical Component for Ensuring Software Supply Chain Security*

Most commercial and custom software applications contain at least some open source code. Typical vulnerability analysis tools do not inspect the individual open source components within applications, although any of these may contain vulnerabilities or obsolete code that can put your organization at risk. The Log4j vulnerability that enabled the massive cybersecurity attack that spread to SolarWinds customers in 2020 is a perfect example.

## **Cyber Mandates and Directives**

In response to ongoing breaches, multiple international organizations have developed mandates, directives, and guidelines to strengthen software supply chain security and minimize the threat of future attacks.

In the United States, Executive Order 14028 was issued in May 2021. This order defines security measures that must be followed by any software publisher or developer that does business with the federal government. Additionally, in December 2022, the signing of Section 3305 of the Consolidated Appropriations Act of 2023 authorized the Food and Drug Administration (FDA) to establish cybersecurity standards for medical devices.

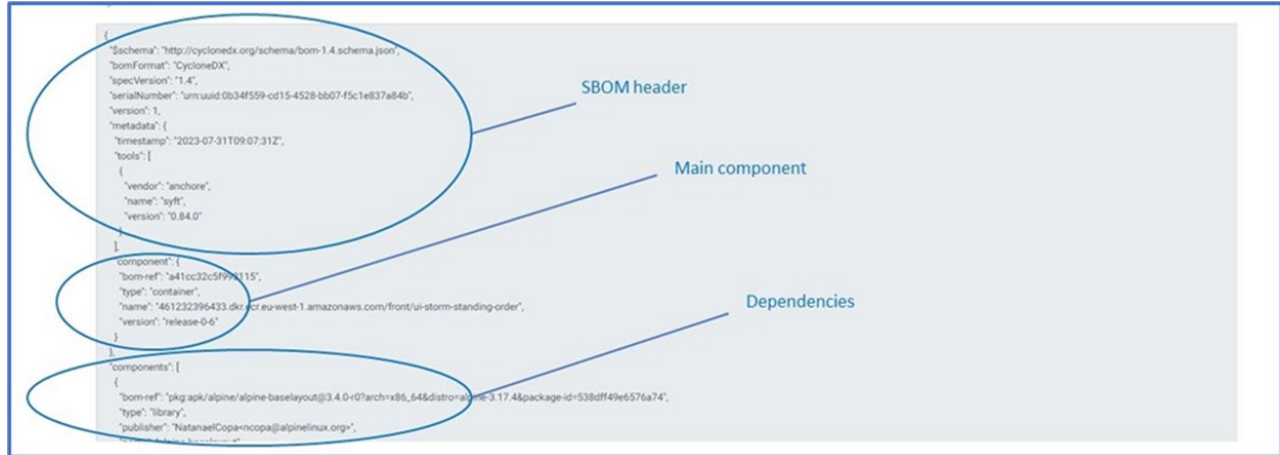
In the European Union, the Network and Information Security (NIS) Directive established EU-wide legislation on cybersecurity. The subsequent NIS2 agreement, put into force in January 2023, obligates more entities and sectors to take measures to increase the level of cybersecurity in Europe.

Specific industries are also enacting guidelines, with the banking and financial sectors taking the lead. The New York State Department of Financial Services' 23 NYCRR500 with Incorporated Second Amendment spells out requirements and compliance measures for financial institutions that are based in or doing business in the State of New York. In the EU, the Digital Operational Resilience Act (DORA) [Regulation (EU) 2022/2554] also defines uniform requirements concerning the security and risk management of network and information systems in the financial industry. These are just a few of the initiatives being developed and enacted.

**One common element of each of these mandates is the use of the Software Bill of Materials, or SBOM.**

## What is an SBOM?

A Software Bill of Materials, or SBOM, is a file that provides an “ingredients list” of all libraries and components that make up an application. It shows the origin or DNA for each piece of code and is typically created by the publisher of the software.



SBOMs provide information that can help organizations solve challenges around:

- Vulnerability Management
- Open Source Software Risks, and
- Mandates and Directives.

## Minimizing Open Source Software Risks

Using open source software introduces multiple types of risk to an organization:

1. **Vulnerabilities** - Any library or component may contain potential vulnerabilities that provide access for hackers. Legacy vulnerability scanning tools do not look for potential issues “behind the scenes” within applications.
2. **Obsolescence** - Older open source code may be obsolete and overlooked. Undermanaged code of this sort can also invite hacking activity.
3. **Licensing Risk** - Open source code is licensed in numerous ways, defining how it may be utilized in software applications. Permissive licenses allow for the code to be used in many ways with few (or no) limitations. More restrictive license types, such as Strong Copyleft, outline limitations of how the code may be utilized, what type of credit must be given to the developer, and more. If these conditions are not met, users may be forced to share their IP, or they may be subject to other legal and financial penalties.

While open source licensing is primarily a concern for commercial publishers and in-house application development teams, it is prudent for organizations acquiring third party software to review the SBOMs for products they plan to acquire to minimize the risk of problems appearing later around licensing. This is also a prime opportunity to check for potential vulnerabilities as well.

## **SBOM Manager™**

Eracent's SBOM Manager™ is a standalone module of the Cybersecurity Management Suite™ (CSMS). SBOM Manager provides a well-rounded set of data, reporting and analysis features that help organizations minimize risks and comply with cyber mandates and directives.

While SBOM Manager provides value to in-house and commercial application development teams, it is also unique in its approach to meeting the requirements of organizations that purchase or subscribe to software from numerous publishers. These “software consumers” will have to manage dozens, hundreds, or even thousands of SBOMs for products that they use, and this is impractical or impossible to do one SBOM at a time.

SBOM Manager is based around a centralized, single-source repository of libraries, components, and other related data from SBOMs. It saves considerable time when a vulnerability is reported since it eliminates the need to review SBOMs individually.

### ***How does SBOM Manager work?***

Customers upload their SBOM files via the user interface. During this straightforward process, users can assign related information that can be used to support reporting, filters, data access, and more. This information includes Publisher, Line of Business, Application Component, and more.

The SBOM Manager “deconstructs” each uploaded SBOM and records the software product to which the SBOM belongs and all the SBOM’s content. This results in an index of components and libraries mapped to products. **If a vulnerability is reported by NIST or another organization, customers get an immediate report of every product in use in their organization that includes the affected component or library.**

SBOM Manager is continuously monitored and updated, and it leverages vulnerability data from NIST and other trusted global sources. It uses this data to display risk scores, levels of criticality, and more.

SBOM Manager also provides visibility into license types for each component and library, reducing the risk of unknowingly using a library that has excessive restrictions when less risky options are available. The system offers version tracking – the version in use, newer available versions, and version history – as well as lifecycle dates that support obsolescence management.

The dedicated open source library within Eracent's IT-Pedia® product data library provides a solid foundation for SBOM Manager's analysis and reporting.

## **Eracent's Cyber Security Management Suite™ (CSMS)**

The Cyber Security Management Suite is a framework-based, proactive process management solution. It provides guidance and governance that enables organizations to successfully implement and maintain a NIST-compliant cybersecurity program that provides results.

The CSMS system aligns existing tools, people, and processes, ensuring full coverage of all assets and endpoints. It also provides continuous progress metrics and a means of assigning ownership and accountability to activities, including policies and mitigation steps.

Mapping of every asset to related systems and landscapes provides a context and potential impact assessment, and aggregate risk scoring is supported. Role-based security supports varied access and data views, and dynamic reporting offers CISOs and cyber team members the exact information that they need to make informed and effective decisions.

To learn more about SBOM Manager and the Cyber Management Security Suite, contact Eracent today!

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

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

**eracent.com**