sonatype

CHEAT SHEET

What is a software bill of materials (SBOM)?

A software bill of materials (SBOM) is a comprehensive list of all packages, libraries, and **dependencies** in a software application.

Beyond its use as an inventory of components, an SBOM provides transparency that is crucial for identifying **security vulnerabilities**, managing risks associated with open source components, and addressing license issues. As cyberattacks on **software supply chains** increase, an SBOM becomes an essential first step in preemptive risk management and security planning.

Why do I need an SBOM?

An SBOM is essential for:

- Ensuring consistent, up-to-date documentation of software dependencies.
- Simplifying the review and automation of dependency management.
- Standardizing dependency information across ecosystems, enhancing security and consistency.
- Providing transparency for consumers, ensuring compliance with security requirements, and facilitating risk assessment with tools for **vulnerability scanning**.

What are the minimum requirements for an SBOM?

The minimum SBOM requirements focus on critical data fields for component tracking and robust automation support:

- **Data fields:** Include supplier and component names, version, dependency relationships, author, and data addition time.
- **Automation support:** Facilitates SBOM generation and parsing for interoperability without requiring new tools.

This streamlined approach ensures that essential information is captured and shared efficiently across organizations.

What are SBOM formats?

SBOM formats provide structured methods to convey software components' details.

Recognized by the National Telecommunications and Information Administration (NTIA), key formats include:

- **CycloneDX:** An open source standard focused on cybersecurity, designed for seamless integration into build pipelines, emphasizing vulnerability and license tracking.
- **SPDX:** This format streamlines package data sharing and is recognized internationally, helping to minimize redundancies and enhance distribution and compliance efforts.
- **SWID Tags:** Software identification (SWID) tags offer a framework for software asset management and vulnerability analysis. They support dynamic updates to accurately reflect software changes, streamlining inventory and vulnerability tracking.

Each format has its unique focus and strengths, catering to different aspects of software documentation and management.

How can you enhance SBOMs with Vulnerability Exploitability eXchange (VEX)?

Vulnerability Exploitability eXchange (VEX) enhances SBOM utility by providing these specific insights into vulnerabilities:

- **Targeted analysis:** VEX identifies which vulnerabilities genuinely impact a product and which do not, allowing for precise, actionable security information.
- **Effective communication:** VEX enables software vendors to convey only the relevant risks to users, avoiding unnecessary alerts about non-impactful vulnerabilities.
- **Operational efficiency:** VEX helps streamline security data management, ensuring that vulnerability details remain current and actionable over time.

VEX-based SBOM management provides these targeted insights into the exploitability of documented vulnerabilities and helps sharpen the focus of security practices.