CycloneDX

CycloneDX provides advanced supply chain capabilities for cyber risk reduction.

Overview

CycloneDX is a modern standard for the software supply chain. CycloneDX Bill of Materials (BOM) can represent full-stack inventory of software, hardware, services, and other types of assets. The specification originates and is led by the OWASP Foundation, standardized by Ecma International, and supported by the global information security community.

Cybersecurity

With CycloneDX, security risks can easily be identified and communicated for effective vulnerability management. Its' use of Package URL, CPE, and SWID makes it ideal for use in vulnerability response, GRC, and CMDB systems. Comprehensive support for services provides insights into the potential attack surface of applications or systems. And leveraging provenance, pedigree, and formulation data provides opportunities for in-depth discovery of cyber risks.

360˚ License Compliance

CycloneDX provides advanced license support incorporating SPDX license IDs and expressions and robust commercial licensing support essential for procurement, cybersecurity, and enterprise Software Asset Management (SAM) use cases. Only CycloneDX delivers complete license coverage to enable your organization, team, or open source project to achieve its' license compliance goals.

The CycloneDX Advantage

- Easy to adopt, implement, and extend
- Official guides that provide insights and best practices for rapid adoption and optimization
- Extensive catalogue of available tools
- Single standard supporting everything necessary for complete software and system transparency
- Discover and engage with the world's largest community of SBOM adopters, supporters, and enthusiasts
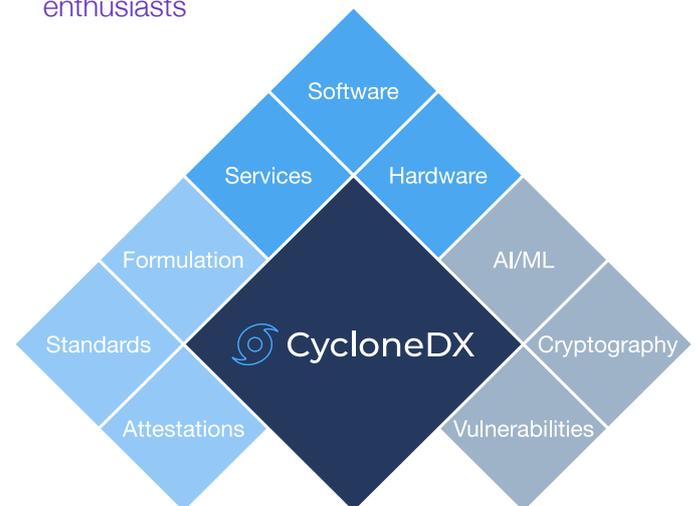
U.S. Executive Order 14028

CycloneDX is an ideal choice for compliance with Executive Order 14028 as it exceeds all SBOM requirements defined by NTIA while also helping agencies achieve the cryptography requirements in National Security Memorandum (NSM-10) for quantum-safe systems and applications.

Visit cyclonedx.org to learn how your organization, team, or open source project can easily adopt and optimize the use of SBOMs.