Introduction to Ecma TC54

Specifications for Software and System Transparency

TC 54 Software and System Transparency

Standardizing core data formats, APIs, and algorithms that advance software and system transparency ecma INTERNATIONAL

OWASP®

Specifications

TC 54	Standardize core data formats, APIs, and algorithms that advance software and system transparency. TC54 standardizes OWASP CycloneDX along with proposals developed by the individual Technical Groups.	CycloneDX
TG1	Develop and maintain a standardized, format-agnostic API that enables the efficient discovery and exchange of Bills of Materials (BOMs) and other related artifacts and intelligence between systems.	Transparency Exchange API
TG2	Develop and maintain the Package URL specification. TG2 also standardizes the VERS specification for uniform version ranges and establishes an ongoing review process and governance for new PURL types.	Package-URL and VERS
TG3	Develop the Common Lifecycle Enumeration (CLE) supporting component aliasing, component lifecycle events such as end-of-life (EOL) and end-of-support (EOS), and provenance chaining over time.	Common Lifecycle Enumeration
TG4	Develop contributing.yaml, a specification for signaling the state, support levels, and needs of open-source projects. It enables transparency into project viability, supports contributor matching, and improves ecosystem sustainability.	NEW Contributing.yaml

CRA Relevance of TC54

- **Global Standardization of SBOM**

  TC54 standardises OWASP CycloneDX as ECMA-424, aligning SBOM requirements with CRA's call for transparency across the software supply chain.

- **Beyond SBOM – Broader Transparency Artifacts**

  TC54 develops related standards (e.g., TEA, CLE, PURL, VERS) that directly address CRA obligations for software lifecycle, vulnerability, and risk transparency.

- **Industry and Community Consensus**

  Brings together vendors, open source, and regulators to converge on consensus-driven standards.

- **Secure by Default Enablement**

  TC54 standards support CRA obligations for secure development practices, by defining machine-readable artefacts for attestations, claims, and evidence.

CRA Relevance of TC54

- **Future-Proofing Regulatory Needs**

  Actively expanding coverage into attestations, cryptography BOMs, algorithm enumerations, and sustainability, ensuring CRA alignment as requirements evolve.

CycloneDX Bill of Materials Standard

Introduction and Roadmap

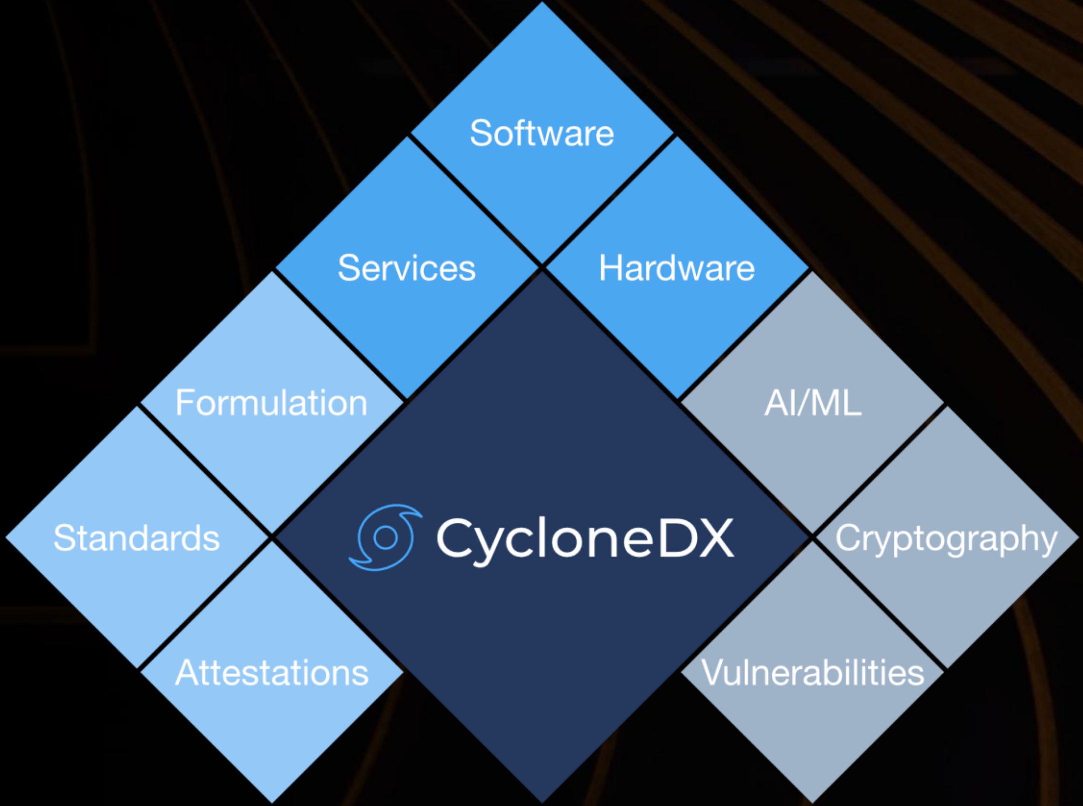
CycloneDX is a Full Stack BOM Standard

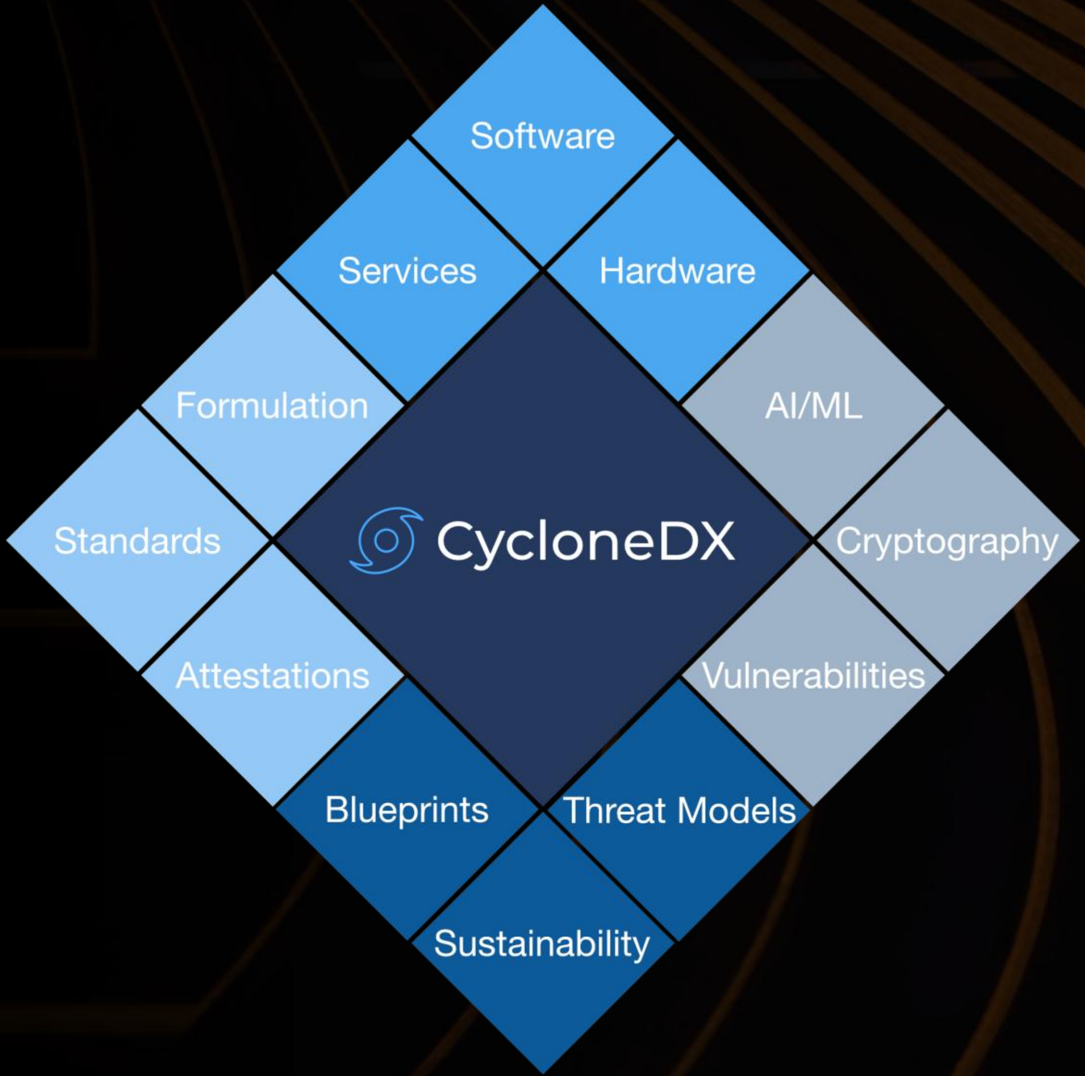
Provides advanced supply chain capabilities for cyber risk reduction

In Production! At an estimated 100K organizations

Estimated **3B** components represented monthly

SaaS


Software
Services
Hardware
Formulation
AI/ML
Standards
CycloneDX
Cryptography
Attestations
Vulnerabilities



Software

Services

Hardware

Formulation

AI/ML

Standards

CycloneDX

Cryptography

Attestations

Vulnerabilities

Blueprints

Threat Models

Sustainability

Features Coming to v1.7

- Support for Patents and Patent Families
- Improvements to Cryptography Support (CBOM)
- Traffic Light Protocol (TLP) Support
- ...more

v1.7 is expected to be ratified in December 2025

Features Coming to 2.0

- Modular Design
- Support for Blueprints (models)
- Support for Representing Complex Threat Models
- Support for Behaviors
- …more

v2.0 is planned for ratification in 2026

Common Lifecycle Enumeration

Track Product Lifecycle Events and Milestones

Why CLE is Needed

- Fragmented Lifecycle Practices
- Risk & Compliance Management
- Component Aliasing & Identity Tracking
- Provenance & Supply Chain Assurance
- Automation & Tooling Enablement
- Cross-Domain Applicability

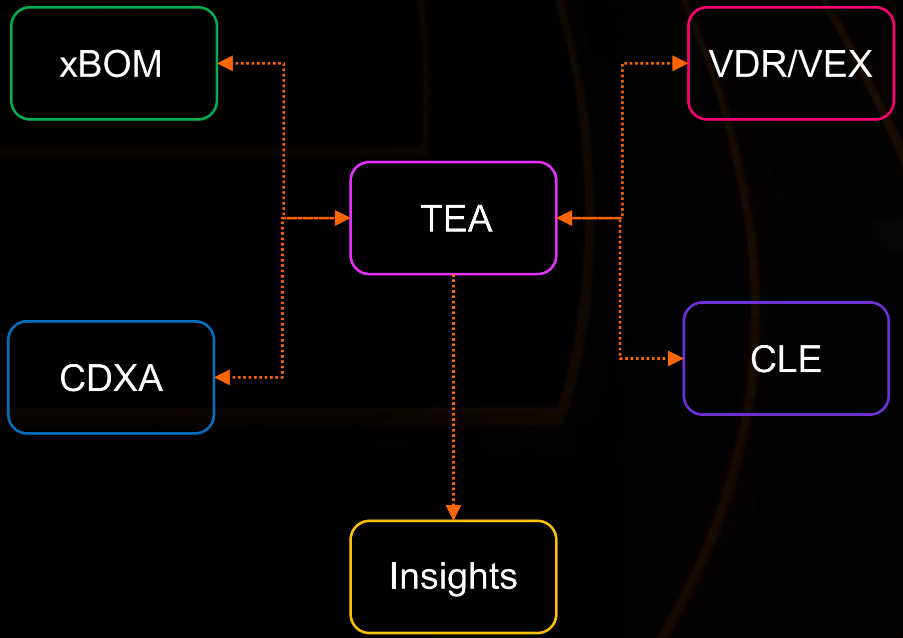
What CLE Captures

- Core Milestone Events
- Support & Maintenance Events
- Identity & Provenance Events

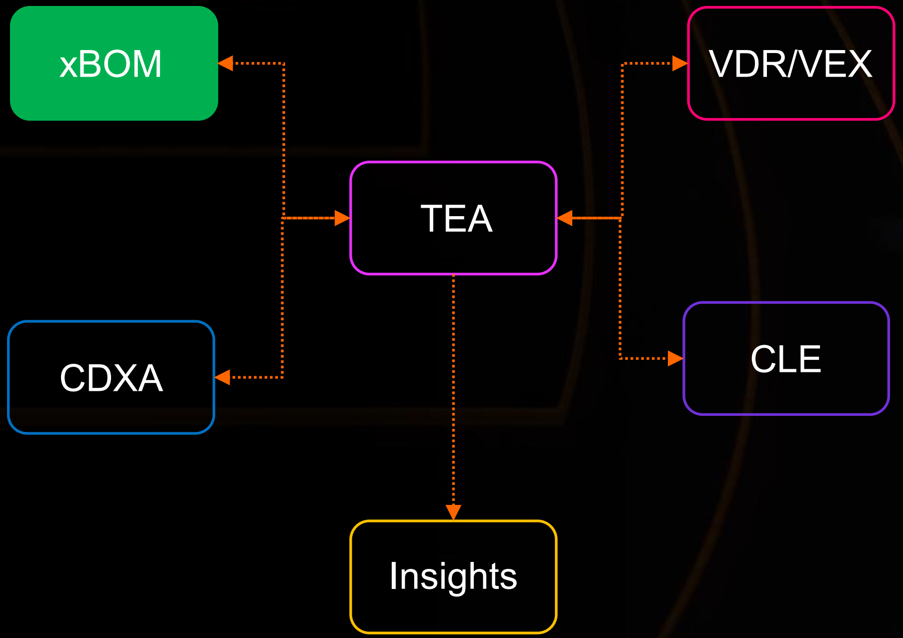
CLE v1.0 is expected to be ratified in December 2025

Transparency Exchange API

Share Supply Chain Artefacts and Intelligence

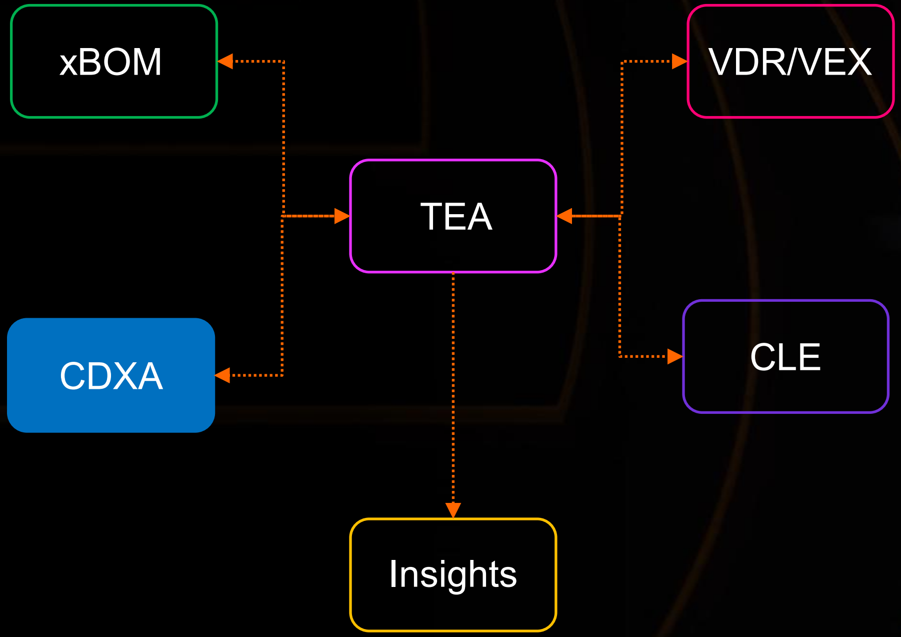


… defines a standard, format agnostic, API for the discovery and exchange of BOMs and supporting material between systems. The core problem here is to discover a set of artefacts based on a product and version identifier for a given product. The API also provides functionality for publishing artefacts with or without signatures.



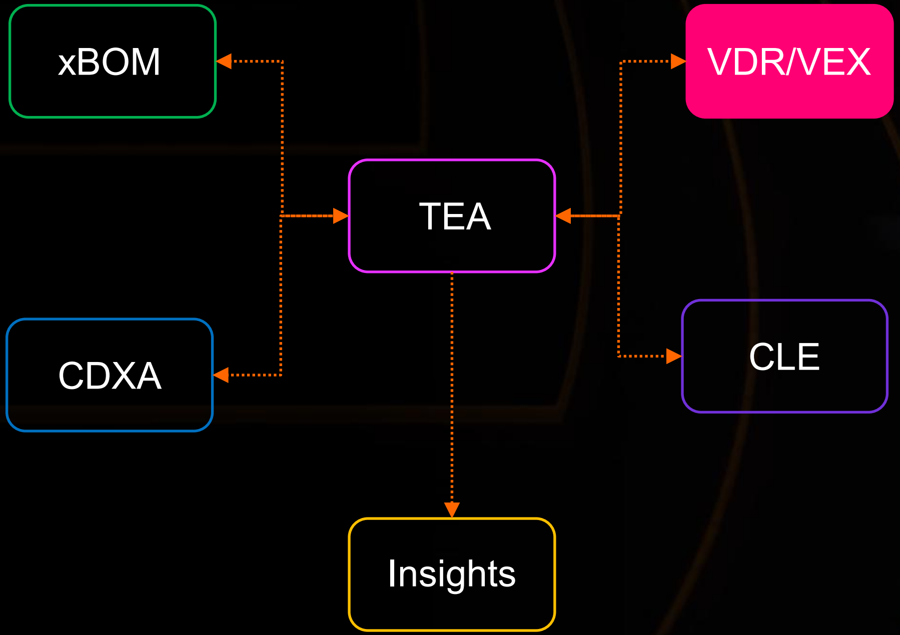
xBOM

Bill of materials for any type of component and service are supported. This includes, but is not limited to, SBOM, HBOM, AI/ML-BOM, SaaSBOM, and CBOM. The API provides a BOM format agnostic way of publishing, searching, and retrieval of xBOM artefacts.



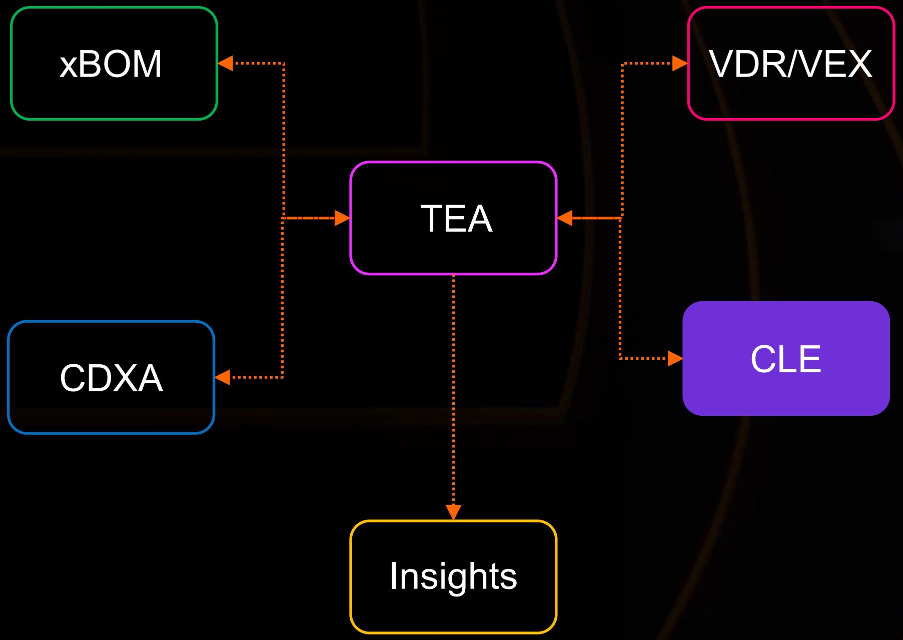
CDXA

Standards and requirements along with attestations to those standards and requirements are captured and supported by CycloneDX Attestations (CDXA). Much like xBOM, these are supply chain artefacts that are captured allowing for consistent publishing, searching, and retrieval.



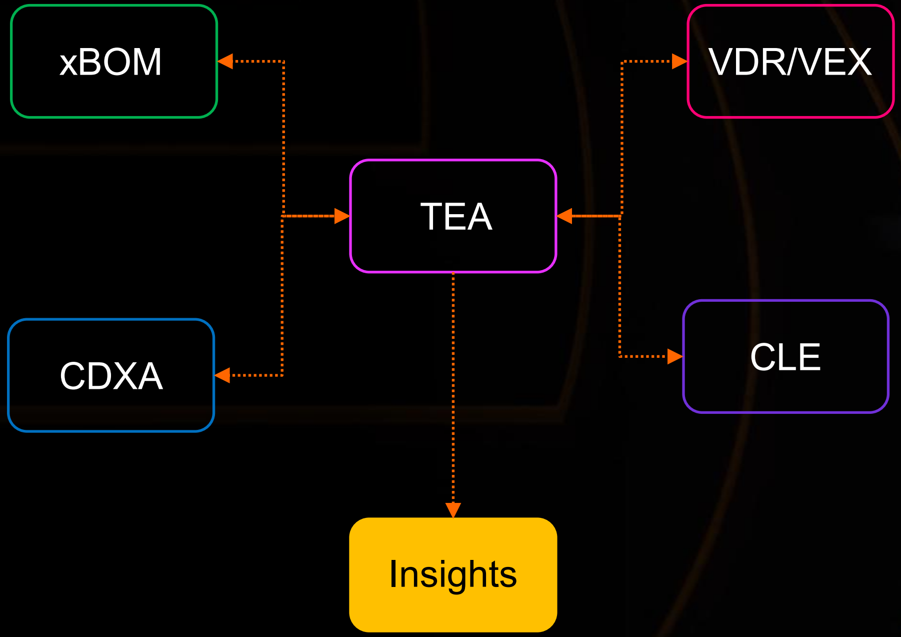
VDR/VEX

Vulnerability Disclosure Reports (VDR) and Vulnerability Exploitability eXchange (VEX) are supported artefact types. Like the xBOM element, the VDR/VEX support is format agnostic. However, CSAF has its own distribution requirements that may not be compatible with APIs. Therefore, the initial focus will be on CycloneDX (VDR/VEX) and OpenVEX.



CLE

Product lifecycle events that are captured and communicated through the Common Lifecycle Enumeration will be supported. This includes product rebranding, repackaging, mergers and acquisitions, and product milestone events such as end-of-life and end-of-support.



Insights

Much of the focus on Software Transparency centers around the concept of “full transparency”. Consumers often need to ingest, process, and analyze SBOMs or VEXs just to be able to answer simple questions such as:

- Do any of my licensed products from Vendor A use Apache Struts?
- Are any of my licensed products from Vendor A vulnerable to log4shell and is there any action I need to take?

Insights allows for “limited transparency” that can be asked and answered using an expression language that can be tightly scoped or outcome-driven. Insights also removes the complexities of BOM format conversion away from the consumers.

Package-URL

Identify and Locate Software Packages

ecma INTERNATIONAL

Q&A

INTERNATIONAL

Rue du Rhône 114
CH-1204 Geneva
T: +41 22 849 6000
F: +41 22 849 6001

www.ecma-international.org