Transparency Exchange API

Introduction, Kickoff, and Contributing

OWASP FOUNDATION

Project Koala

Transparency Exchange API

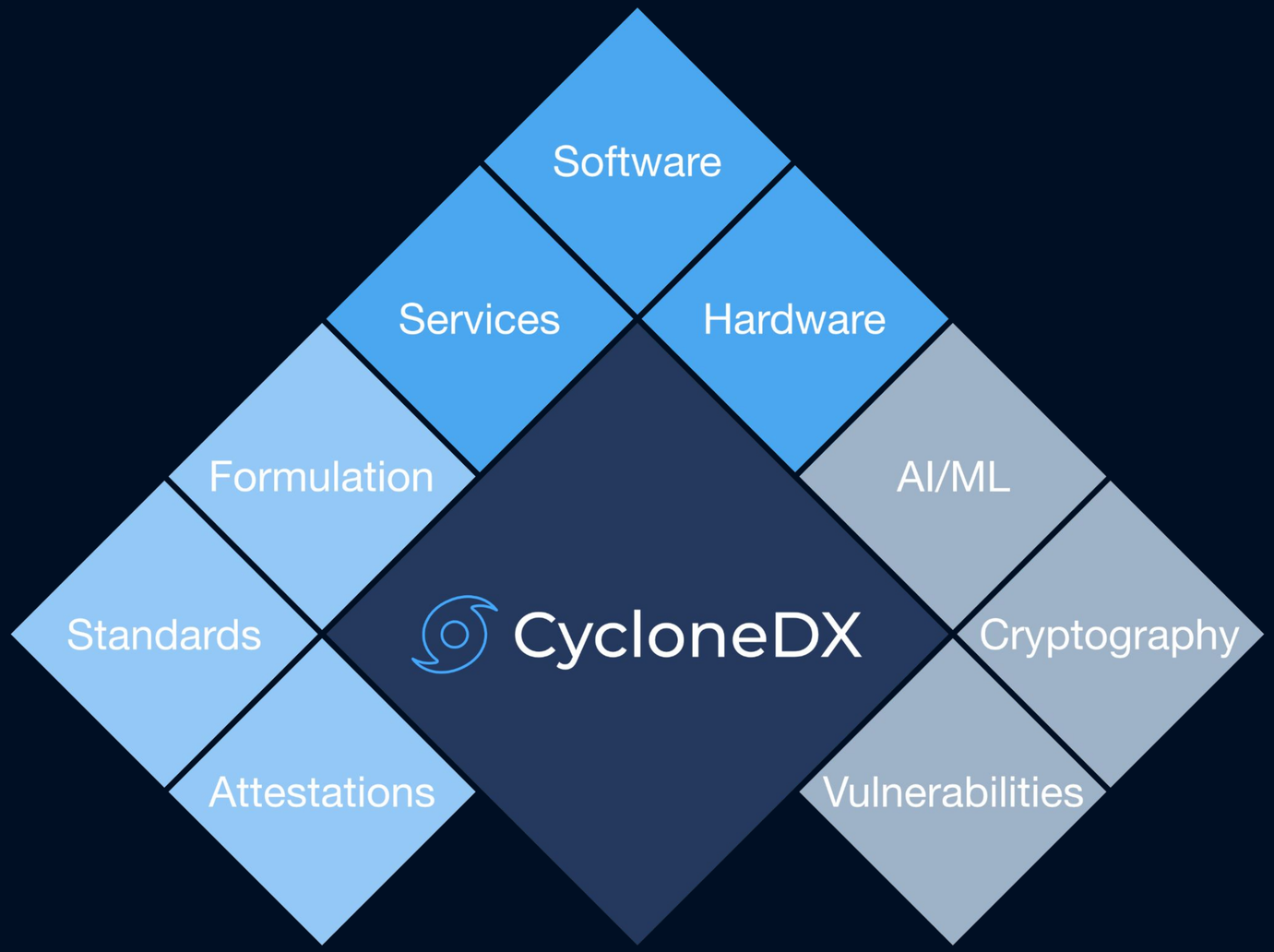
Introduction, Kickoff, and Contributing

OWASP

OWASP FOUNDATION

History

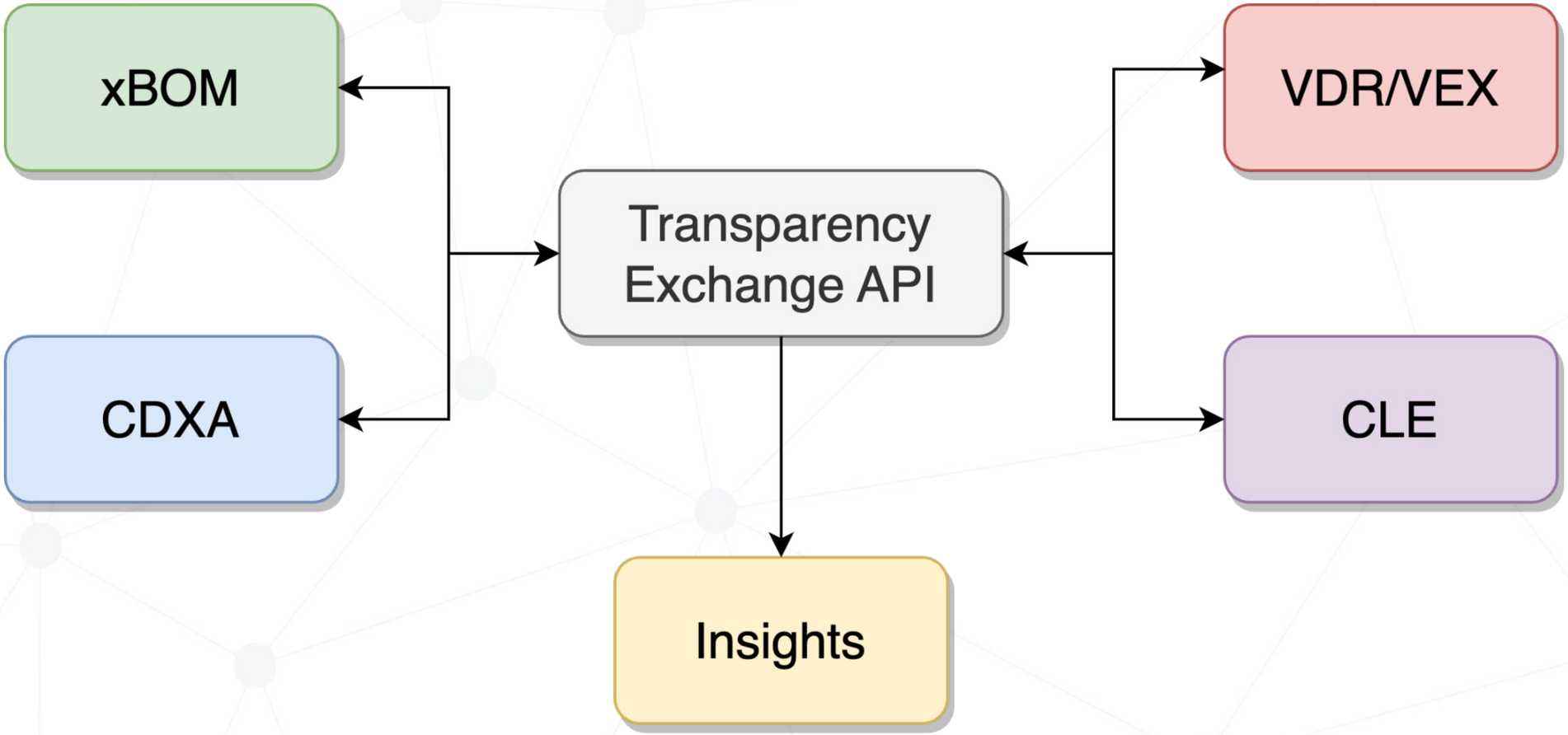
- Started January 2022
- Project Koala (aka: BOM Exchange API)
  - https://github.com/CycloneDX/transparency-exchange-api
- Focused solely on the exchange of BOMs
- Reference implementation
  - https://github.com/CycloneDX/cyclonedx-bom-repo-server


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

Updated Objectives

- Discoverable
- Autonomously automatable
- Fully realize “Software Transparency”
  - Exchange software supply chain artifacts and intelligence
  - Configurable and variable extent of transparency
- Standardization by way of OWASP ➟ Ecma ➟ ISO

Proposed Capabilities



Use Cases Document

THIS DOCUMENT IS CURRENTLY IN DRAFT AND ACTIVELY BEING WORKED ON

Transparency Exchange API

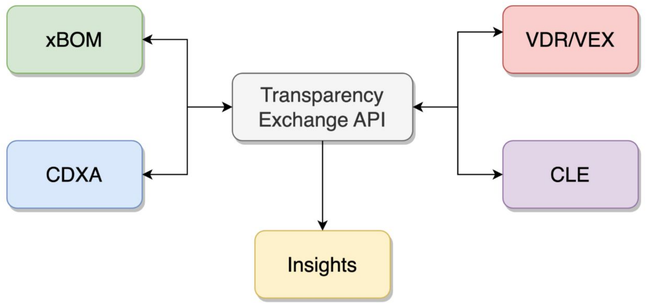
Project Koala

OWASP Workgroup	Project Koala FWG
Ecma Technical Committee	TC54
Ecma Task Group	TBD
Meeting Invite	Google Calendar Link

This specification 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 artifacts based on a product and version identifier for a given product.

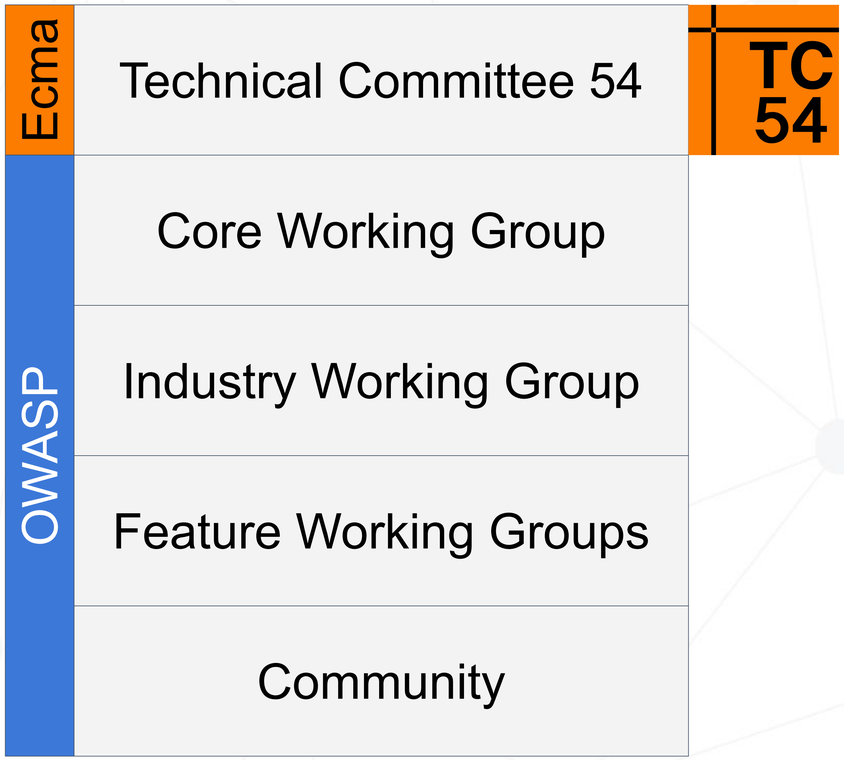
The API should where possible be based on existing solutions, protocols and APIs.

Some of the data in these artifacts may be sensitive for distribution outside of a customer base, or may need a NDA contract for access. In order to enable that kind of control of distribution access control support is needed. It is important that this can be used in an automated system, i.e. not requiring manual log in through a web browser portal.



https://docs.google.com/document/d/1LPNXZ-LmF4ObzpYyAs51WdUktZuTXpOWI_ssGNOCWXQ/edit

About Standardization and TC54



https://tc54.org/

Software and System Transparency

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

- CycloneDX
- Package URL
- Transparency Exchange API

Other considerations

- Common Lifecycle Enumeration

Participation

- OWASP initiatives are open to anyone
- Everyone has an equal seat at the table
- Output will be promoted to Ecma TC54
- Work group meetings start on
  - April 10 from 9am - 10am (US Central / 2pm UTC)
  - Meetings every other week

https://calendar.google.com/calendar/u/0/event?action=TEMPLATE&tmeid=NzdoOWZzOXQxaW92M2ZsYWRqaGw2NHI0NGJfMjAyNDA0MTBUMTQwMDAwWiBjXzg4NGRlY2RlNWExNTI5MDJiYjUxYTYyZjg5NTUwZDBmMzc0ODQ4NDUzNGYwOGM2Mzc5MmYyZTY1NGYyYTdlYmNAZw&tmsrc=c_884decde5a152902bb51a62f89550d0f3748484534f08c63792f2e654f2a7ebc@group.calendar.google.com&scp=ALL