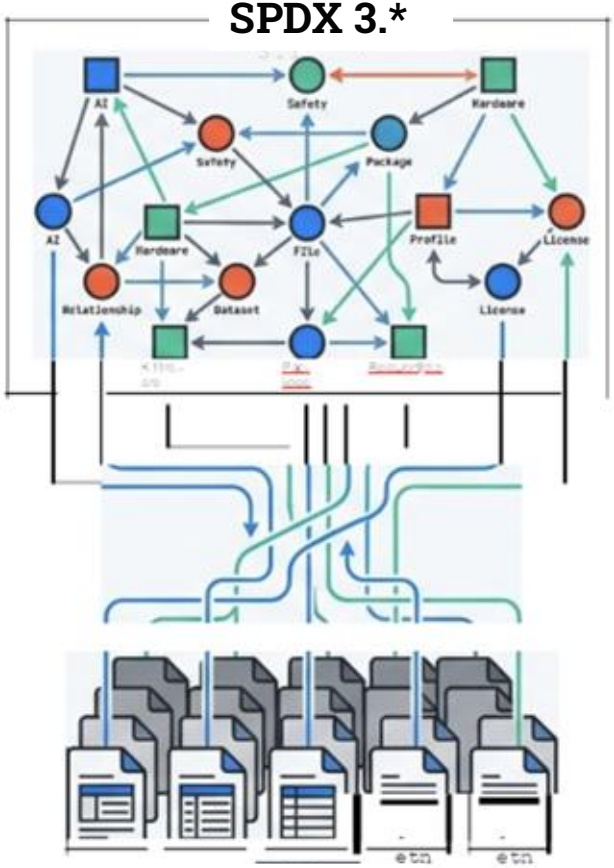
What's new in SPDX 3.1: Supporting a Living Knowledge Graph

Karen Bennet
Co-chair SPDX AI/Dataset Profile
AI Expert, Standards Council of Canada
ISO A SC42, IEEE AI Committees
30+ Years experience: OSS, AI/ML, Gen AI and Agentic AI systems.

SPDX 3.*


AI
Safety
Hardware
Safety
Package
AI
Hardware
File
Profile
License
Relationship
Dataset
License

SPDX 2.*

SPDX v3.1-RC1 Specification

https://spdx.github.io/spdx-spec/v3.1-RC1/

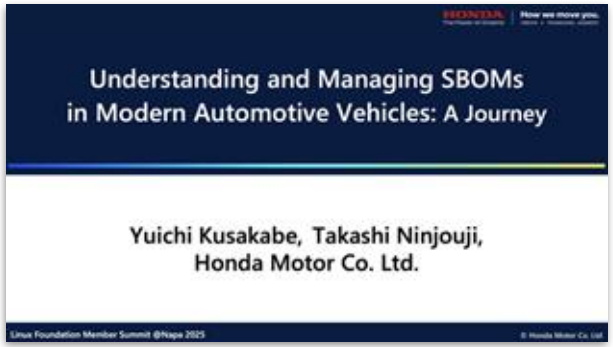
Release Candidate (RC1) is intended for testing and validation.

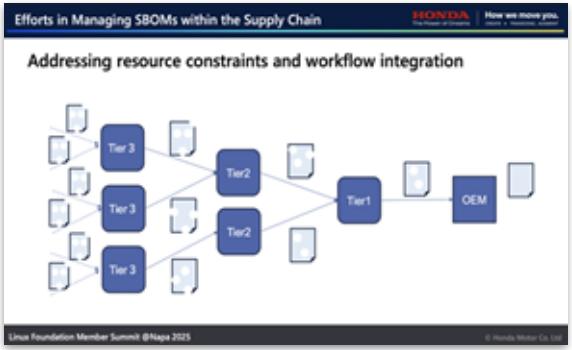
Expands beyond describing metadata on software for products, SPDX now supports a knowledge graph for full supply chain for products & systems in critical infrastructure

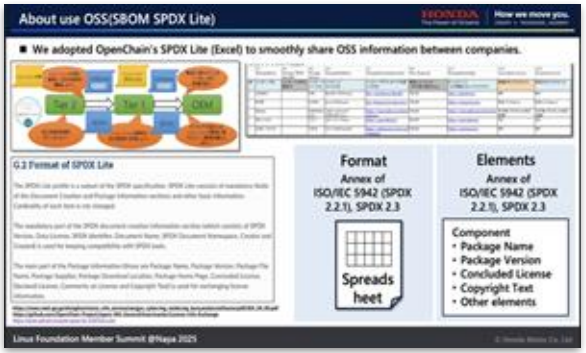
- **New Profiles:** Safety, Service, Hardware, Supply chain, and Operations
- **Updated Profiles:** Security, AI, Dataset, Software and Core
- **RelationshipType** has grown from 59 to 76 entries
- Introducing **SPDX Vetted Cryptography List** similar to SPDX License List

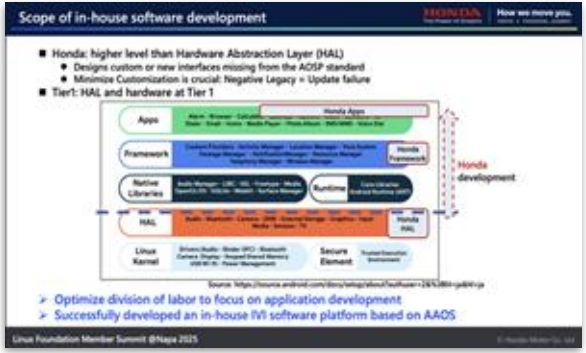
SPDX®

Supply Chain behind a modern car ...

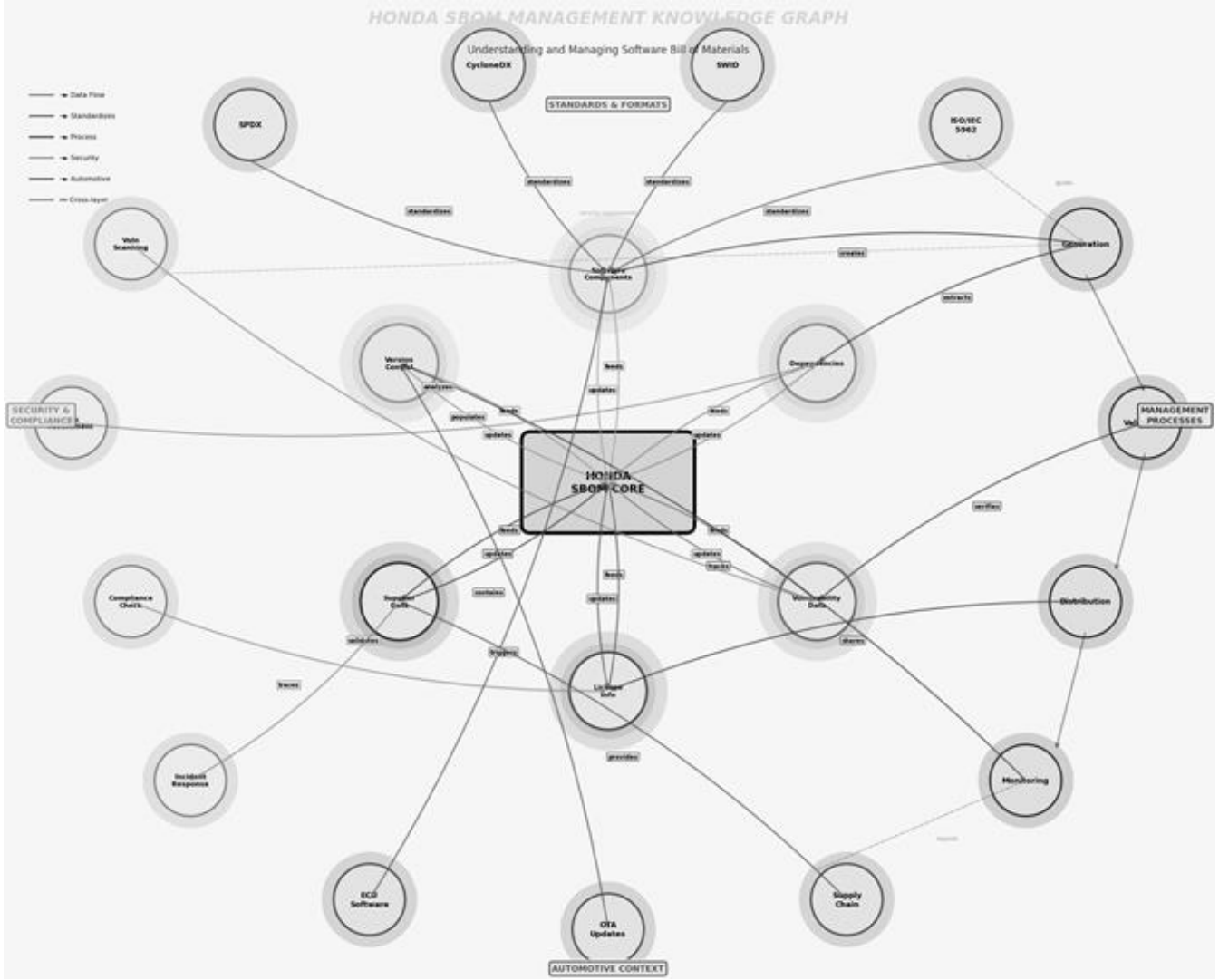








Source:https://static.sched.com/hosted_files/lfms25/e0/250312_UnderstandingandManagingSBOMsinModernAutomotiveVehicles_LFMemberSummit2025.r2.pdf



SPDX®

Self Created Demo of SPDX Knowledge Graph based on Honda's Supply Chain information

SPDX SUPPLY CHAIN

NEW

Actors:

- Organizations
- People

Lifecycle:

Sourcing ➔
Manufacturing ➔
Distributors

Entire network **of organizations, people, activities, information, and resources** involved in the **life cycle of a product or service from creation to end-of-life.**

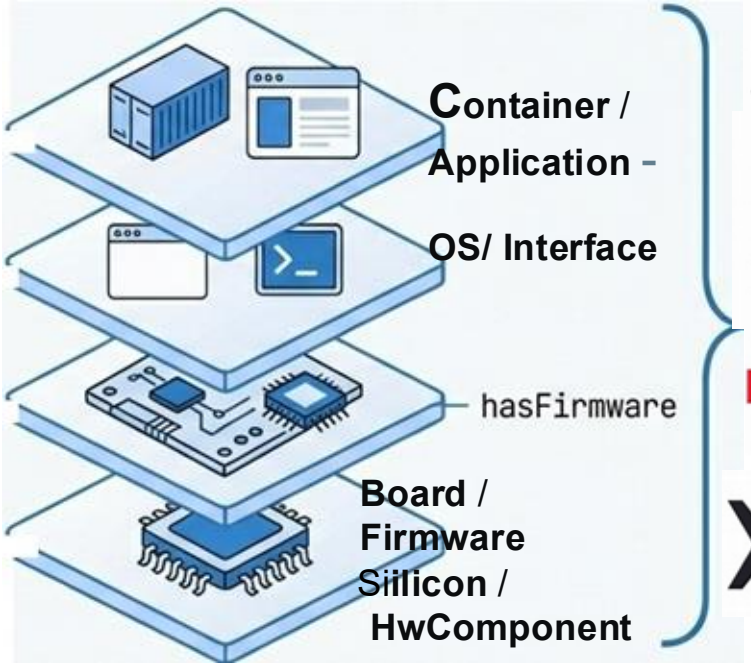
From sourcing inputs and components, through manufacturing and assembly, to storage, distribution, and final delivery to the end user.

SPDX HARDWARE

NEW

Hardware Bill of Materials (HBOM) and hardware-software co-dependencies.

Extend SPDX to encompass physical components, their provenance, and their intricate relationships with firmware and software.



Key Company Contributors

AMD

BOSCH

Microsoft

intel

Honeywell

REFLEX AEROSPACE

.....

SPDX OPERATIONS

NEW

Business context (technical and business operations) of the system such as **Import / Export Control Classification Number** and **Assessments.**

Key Company Contributors

arm

BOSCH

Deloitte.

SPDX SERVICES

NEW

Manage supply chain risks in **cloud-native environments** where traditional package-based SBOMs are insufficient.

- **Service Catalog** - Available services and features
- **Subscription Terms** - Licensing agreements
- **Deployment Config** - Infrastructure as Code (IaC)
- **Usage Metrics** - Resource consumption data
- **Security Posture** - Continuous security monitoring

S**tandardized way of documenting and sharing information** about safety artifacts created, verified and maintained during lifecycle of system.

Set of concepts and data elements related to artifacts and their dependencies that are needed for **system's safety conformance documentation.**

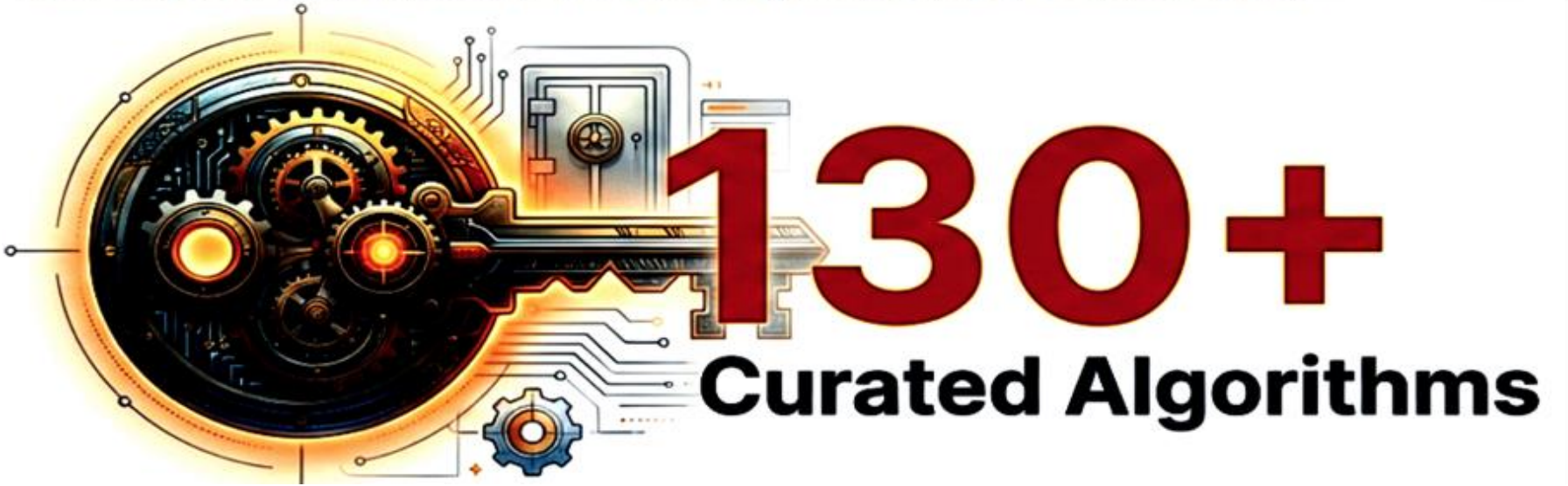
Enables automation of compliance with safety-critical industry standards like automotive (ISO 26262), avionics (DO-178C), medical devices (IEC 62304), and industrial control (IEC 61508)

SPDX CRYPTOGRAPHY

NEW

Standardizing Security: The Curated Cryptography List

SPDX 3.1includes a new, vetted list of cryptographic algorithms to standardize how security mechanisms are documented in the same way it offers the SPDX License List.



Existing Profiles Improvements

- **Consistency**: Field Naming / Metadata captured
- Improved Profile **descriptions, examples**
- Security: Clarify ‘**exploited' property**
- Additional information capture for:
  - **Regulatory Alignment:** such as EU AI Act Readiness, ISO 42001, IEEE 3119-2025
  - **Provenance**

EU CRA Manufacturer Guidance

Work in progress: SPDX-examples/conformance

(SEBoK for Consumer Electronics) includes Stakeholder Needs and Stakeholder Requirements)

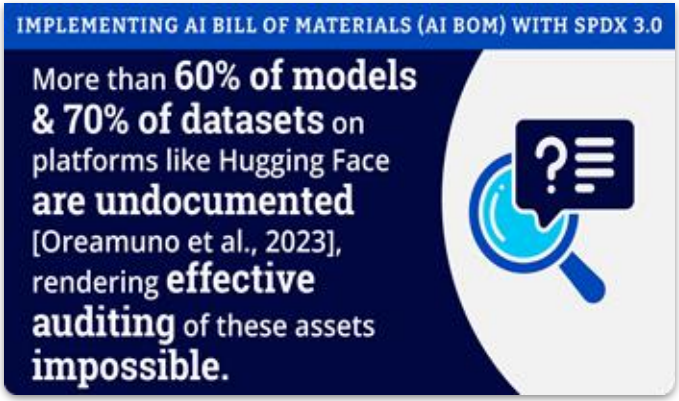
EU CRA Regulatory Knowledge Graph

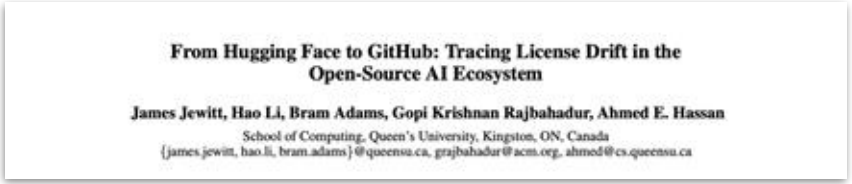
Source: https://openssf.org/blog/2025/10/22/sboms-in-the-era-of-the-cra-toward-a-unified-and-actionable-framework/

Work in progress: Mapping of SPDX fields to CRA clauses/appendix are captured in a spreadsheet

SPDX Tools

SPDX Knowledge Graph Explorer



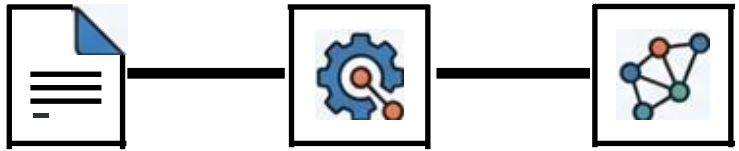


From Hugging Face to GitHub: Tracing License Drift in the Open-Source AI Ecosystem

James Jewitt, Hao Li, Bram Adams, Gopi Krishnan Rajbahadur, Ahmed E. Hassan

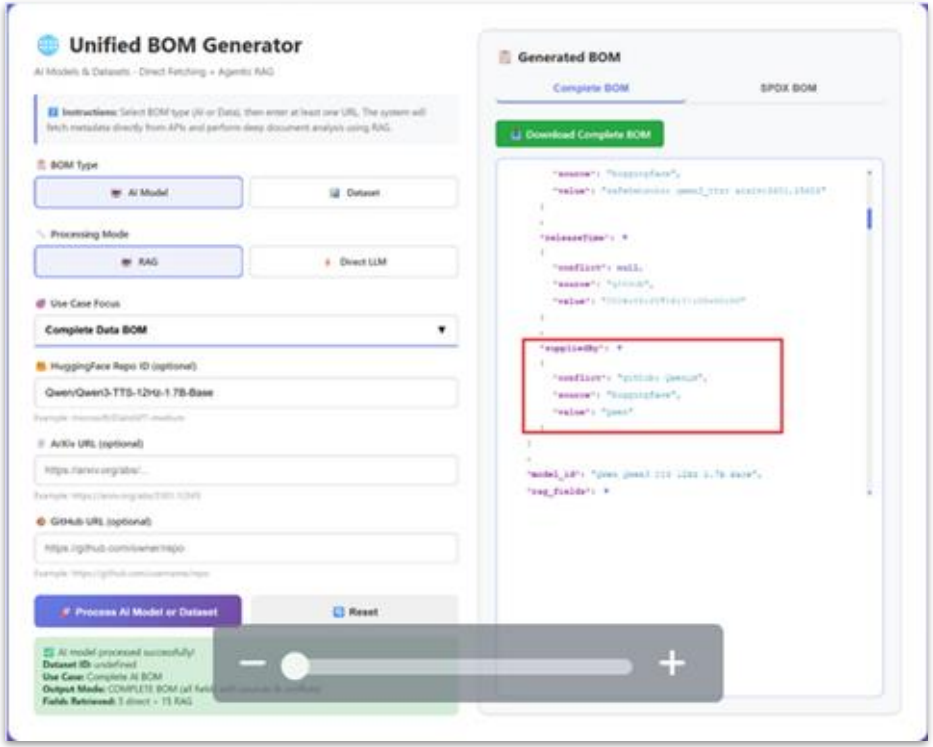
School of Computing, Queen's University, Kingston, ON, Canada
{james.jewitt, hao.li, bram.adams}@queensu.ca, grajbahadur@acm.org, ahmed@cs.queensu.ca

Source: https://arxiv.org/pdf/2509.09873



SPDX

SPDX Knowledge Graph Explorer

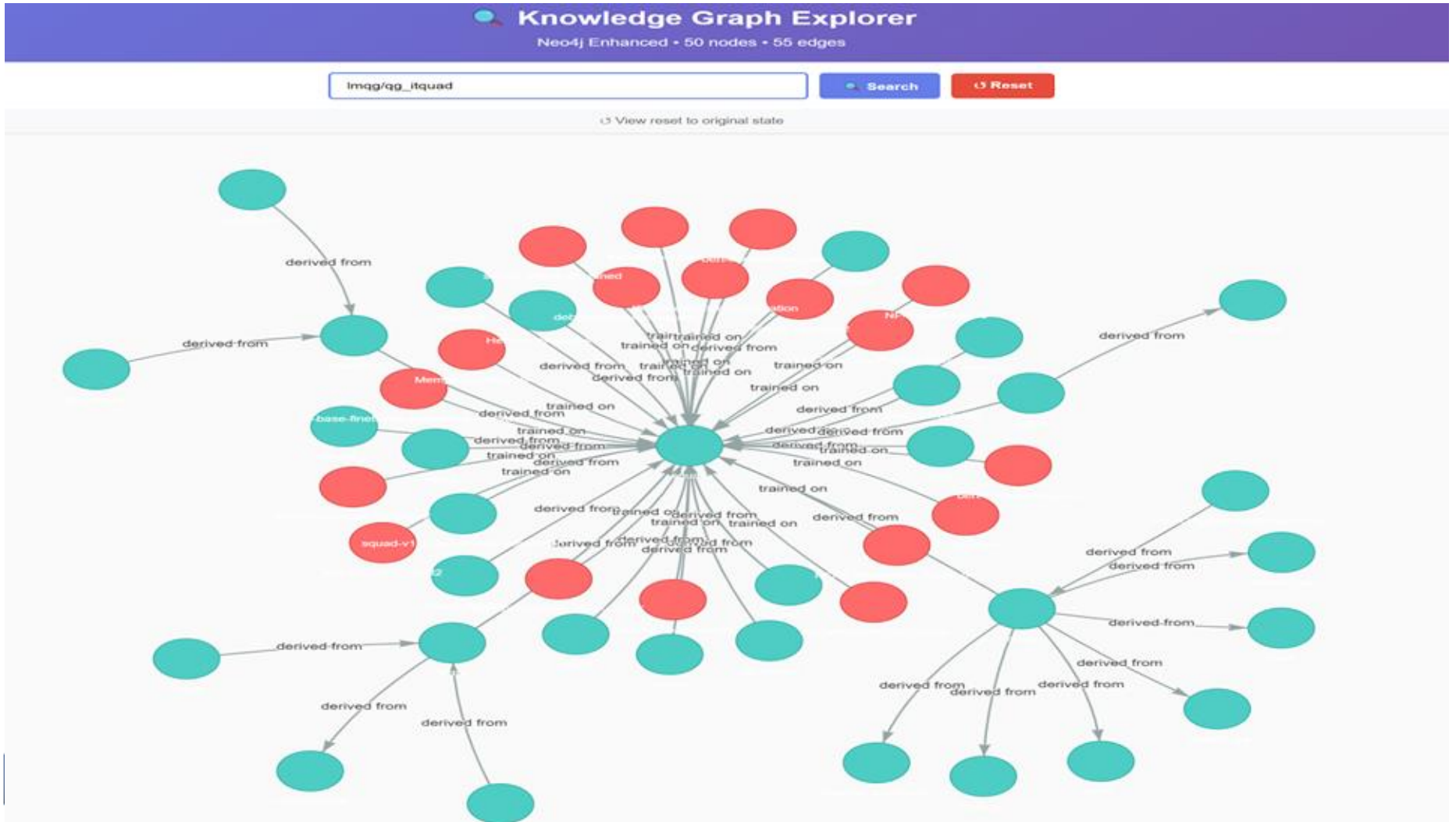


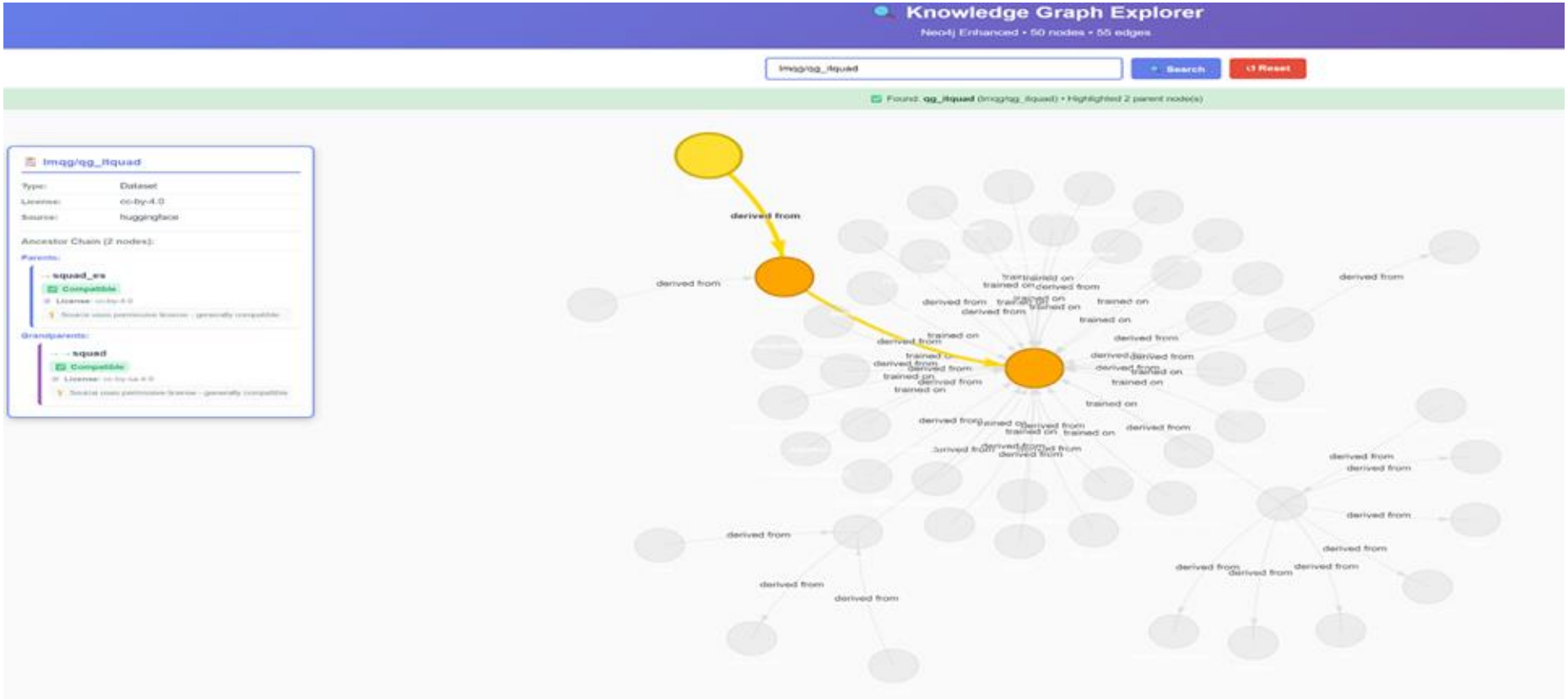
Information Rich Knowledge Graph from multiple sources (source, user guides, hugging face, github, etc).

Generates AI and Dataset BOM that be i**ntegrated into Supply Chain Graph**

Conflict Resolution / Confidence Checker - checks metadata across multiple sources,identifies conflicts like icensing

Demo version available upon request


Knowledge Graph Explorer
Neo4j Enhanced • 50 nodes • 55 edges
lmqg/qg_itquad
Search
Reset
View reset to original state
derived from
trained on
squad-v1


Knowledge Graph Explorer
Neo4j Enhanced • 50 nodes • 55 edges
lmqg/qg_ifquad
Search
Reset
Found: qg_ifquad (lmqg/qg_ifquad) • Highlighted 2 parent node(s)
lmqg/qg_ifquad
Type: Dataset
License: cc-by-4.0
Source: huggingface
Ancestor Chain (2 nodes):
Parents:
squad_es
Compatible
Grandparents:
squad
Compatible
derived from
trained on

SPDX 3.1 Roadmap → RC2

Community Feedback

Addressing community feedback

OWASP Feedback

Strategic Integration

MITRE ATT&CK + D3FEND With Threat and Controls Profile

Scope

Agentic AI

Security

System Engineering

Use Cases .

Continue to prepare Manufacturers for EU CRA

SPDX 3.1 Roadmap → RC2

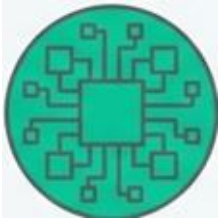
Adding more Real World Examples

Procurement & Auditing

Verifying software bills of materials before purchase.

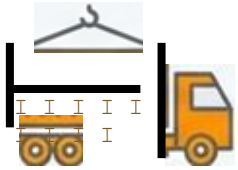
Defense & Hardware

High-security hardware tracking for government contracts.



Semiconductors

Anti-counterfeit tracking and supply chain verification.



Logistics

Real-time monitoring of GPU Shipments.

Come Join Us

Key RC2 Weekly Working Groups

Mondays: Threats and Controls

Tuesday: Tech Team (between Profiles)

Wednesdays: AI / Dataset

Friday: Regulatory Compliance (CRA) & Functional Safety

Resources

SPDX Info: https://github.com/spdx

Guide: OpenChain AI System BOM - Compliance Management Guide for the Supply Chain Wednesdays: AI / Dataset

Whitepaper: Implementing AI BOM with SPDX 3

SPDX

Other SPDX Meetings

SPDX 3.1 Takeaways:

- a **knowledge graph** not just a flat file (although it can export them)

SPDX

https://spdx.github.io/spdx-spec/v3.1-RC1/

SPDX 3.1 Takeaways:

- a **knowledge graph** not just a flat file (although it can export them)
- profiles capture the **full supply chain lifecycle**

SPDX

https://spdx.github.io/spdx-spec/v3.1-RC1/

SPDX 3.1 Takeaways:

- a **knowledge graph** not just a flat file (although it can export them)
- profiles capture the **full supply chain lifecycle**
- provides **Evidence Traceability for Compliance**

SPDX

https://spdx.github.io/spdx-spec/v3.1-RC1/

SPDX 3.1 Takeaways:

- a **knowledge graph** not just a flat file (although it can export them)
- profiles capture the **full supply chain lifecycle**
- provides **Evidence Traceability for Compliance**
- has more Tools to help with **automating the metadata capturing**

SPDX

https://spdx.github.io/spdx-spec/v3.1-RC1/

SPDX 3.1 Takeaways:

- a **knowledge graph** not just a flat file (although it can export them)
- profiles capture the **full supply chain lifecycle**
- provides **Evidence Traceability for Compliance**
- has more Tools to help with **automating the metadata capturing**
- providing more **guides & examples to Help Manufacturers for** compliance such as **EU CRA**

SPDX

https://spdx.github.io/spdx-spec/v3.1-RC1/

Thank You!

Any Questions?