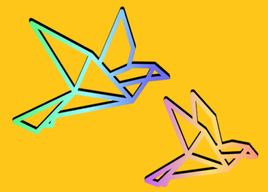


RELIZA

From SBOMs

to xBOMs

to Transparency

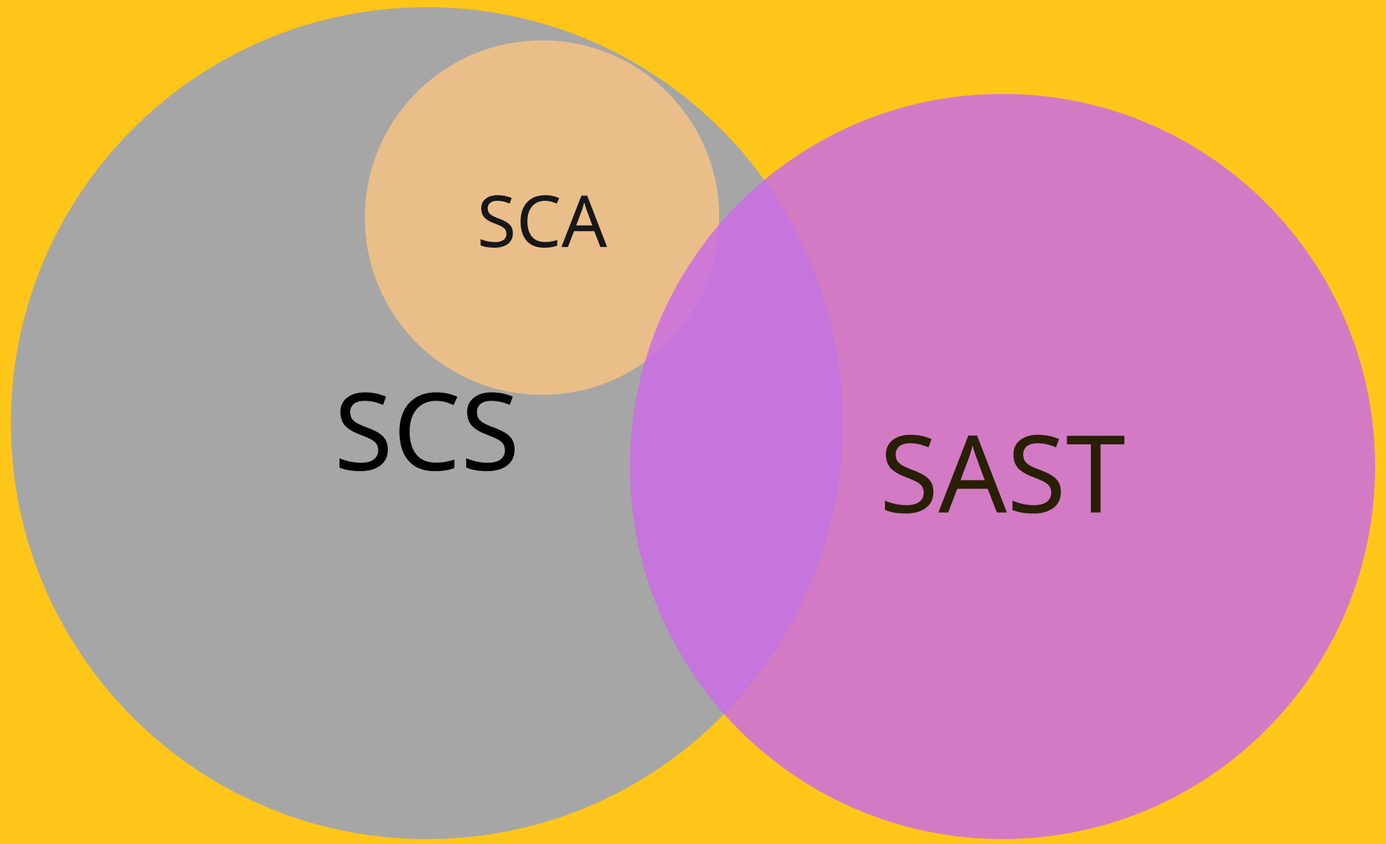
RELIZA

About - Pavel Shukhman

- Founded Reliza in 2019
- Early adopter of CycloneDX
- Vendor supporting CycloneDX
- Building SBOM tooling
- Avid traveler

RELIZA

10,000 Feet View



RELIZA

Notable Supply Chain Attacks

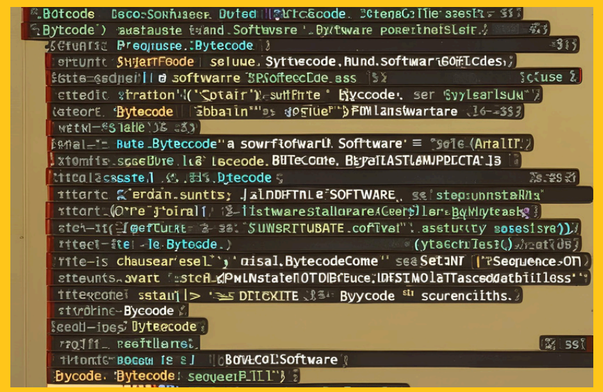
1. NotPetya (2017)
2. SolarWinds (2020)
3. Log4j 0-day (2021)
4. Discord (2024)

RELIZA

Transparency is the Answer to SCS

RELIZA

Source Code / Binary

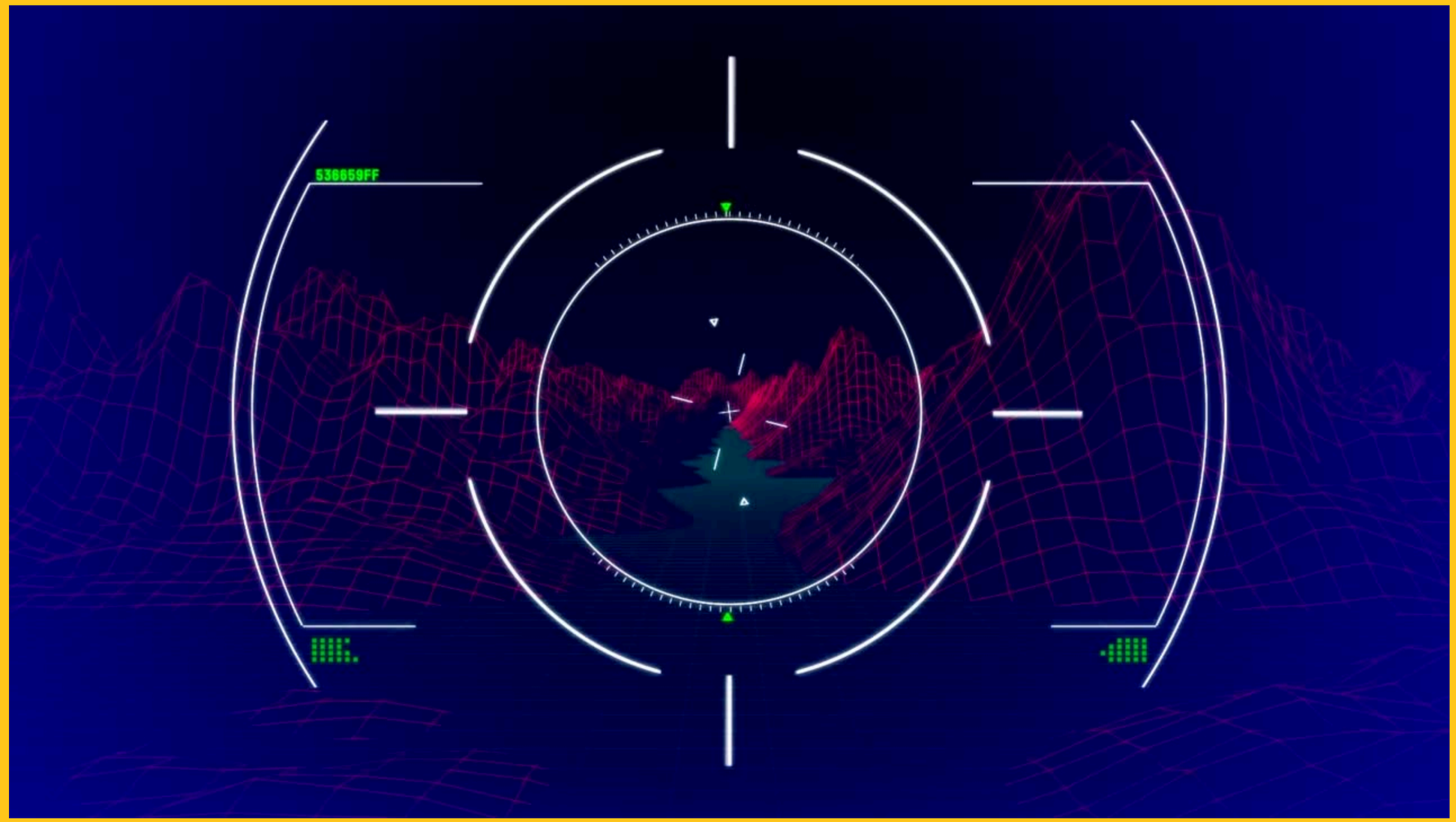


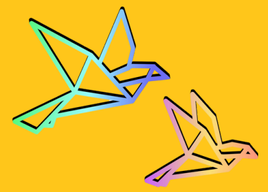
Metadata


```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.6",
  "serialNumber": "urn:uuid:d42ce91e-3ee9-4687-aeaf-75d63d4527e7",
  "version": 1,
  "metadata": {
    "timestamp": "2025-02-23T17:13:32.678Z",
    "tools": {
    "component": {
      "type": "application",
      "name": "Rebom Frontend",
      "version": "1.3.1-3",
      "bom-ref": "pkg:reliza/Reliza Demo/Rebom
      Frontend@1.3.1-3?belongsTo=SCE&hash=84f872c19e56a13c9f47e7447bb090c195066343",
      "purl": "pkg:reliza/Reliza Demo/Rebom
      Frontend@1.3.1-3?belongsTo=SCE&hash=84f872c19e56a13c9f47e7447bb090c195066343",
      "properties": [
      "group": "Reliza Demo"
    }
  },
  "components": [
```

RELIZA

Moving Target

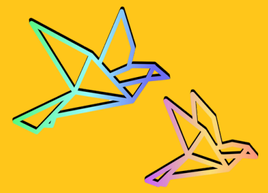




RELIZA

Benefits of Metadata Separation

- Rescans – moving target
- Data querying, exchange, distribution
- Pre-build analysis – shift left
- Compliance, audit – regulatory, legal



RELIZA

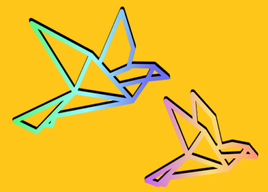
SBOM Standards

CycloneDX

SPDX®

RELIZA

Software Identification

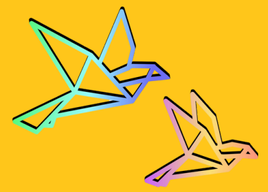


RELIZA

Package URL aka purl

scheme:type/namespace/name@version?qualifiers#subpath

pkg:deb/debian/curl@7.50.3-1?arch=i386&distro=jessie



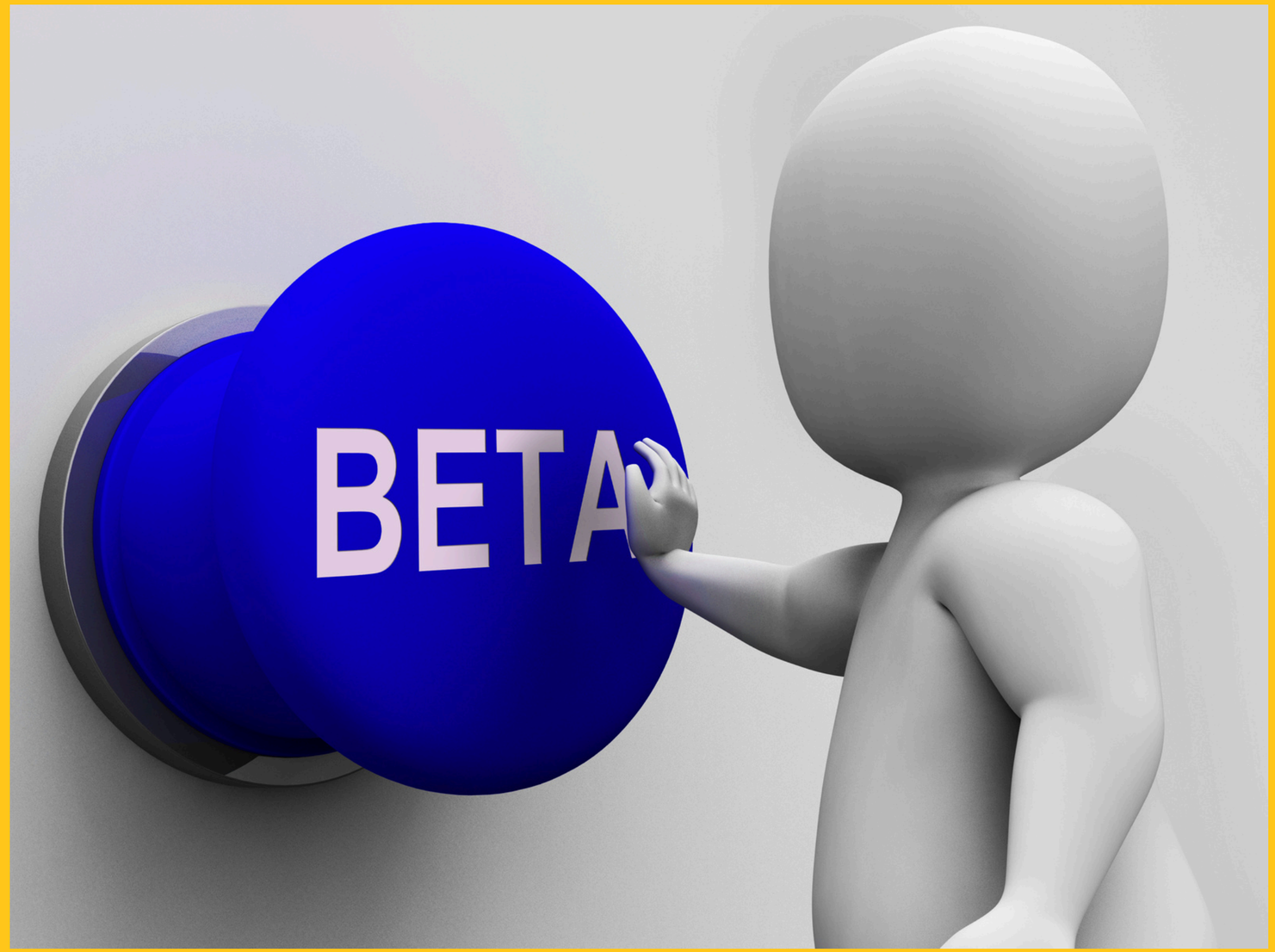
RELIZA

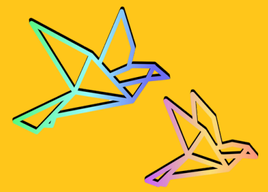
CycloneDX Components

```
100   "components": [
101     {
102       "type": "library",
103       "name": "client",
104       "group": "@apollo",
105       "version": "3.7.12",
106       "bom-ref": "@apollo/client@3.7.12",
107       "author": "packages@apollographql.com",
108       "description": "A fully-featured caching GraphQL client.",
109       "licenses": [
110         {
111           "license": {
112             "id": "MIT",
113             "acknowledgement": "declared"
114           }
115         }
116       ],
117       "purl": "pkg:npm/%40apollo/client@3.7.12",
118       "externalReferences": [
146       "properties": [
152     },
```

RELIZA

Versioning Problem



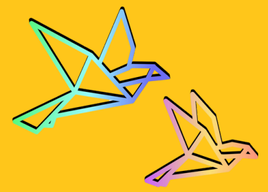


RELIZA

A (mostly) universal version range specifier aka vers

vers:<versioning-scheme>/<version-constraint>|<version-constraint>|...

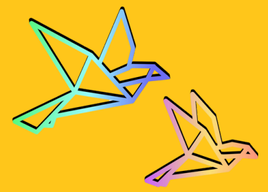
vers:npm/1.2.3|>=2.0.0|<5.0.0



RELIZA

CycloneDX Capabilities - Road to xBOM

- SBOM
- SAASBOM
- CBOM
- HBOM
- ML-BOM
- OBOM
- MBOM
- VDR
- VEX
- BOV
- CDXA
- BOM-LINK
- ...
- ...
- xBOM



RELIZA

Regulatory Pressure

Canada: ISTM.10.071 (2023, Recommendations)

EU: CRA, BSI TR-03183

US: EOs 14028 and 14144, NTIA SBOM Minimum Elements, CISA Framing Software Component Transparency 2024-10

India: SEBI CSCRF

RELIZA

RELIZA

Organizing The Mess

Common Lifecycle Enumeration

xBOMs

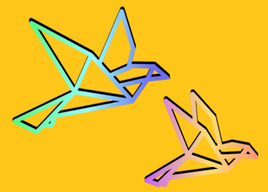
- Design
- Pre-build
- Build
- Post-build
- Operations
- Discovery
- Decomission

Products

- Naming Change
- Versioning Change
- Licensing Change
- Version Events:
  - GA
  - End of Development
  - End of Marketing
  - End of Support
  - Superseded By
  - End of Life

RELIZA

Transparency Exchange API aka TEA



RELIZA

References

- https://cyclonedx.org/
- https://spdx.dev/
- https://github.com/CycloneDX/
- https://github.com/package-url/
- https://github.com/DependencyTrack
- https://worklifenotes.com/2025/01/21/why-we-chose-cyclonedx-over-spdx/
- https://worklifenotes.com/2025/01/14/why-a-single-sbom-is-never-enough/
- https://github.com/CycloneDX/transparency-exchange-api/
- https://worklifenotes.com/2025/02/25/3-dimensions-of-versioning-problem/
- https://github.com/relizaio/rebom
- https://fosdem.org/2025/schedule/event/fosdem-2025-6483-where-in-the-oss-supply-chain-do-sbom-attributes-come-from-/

RELIZA