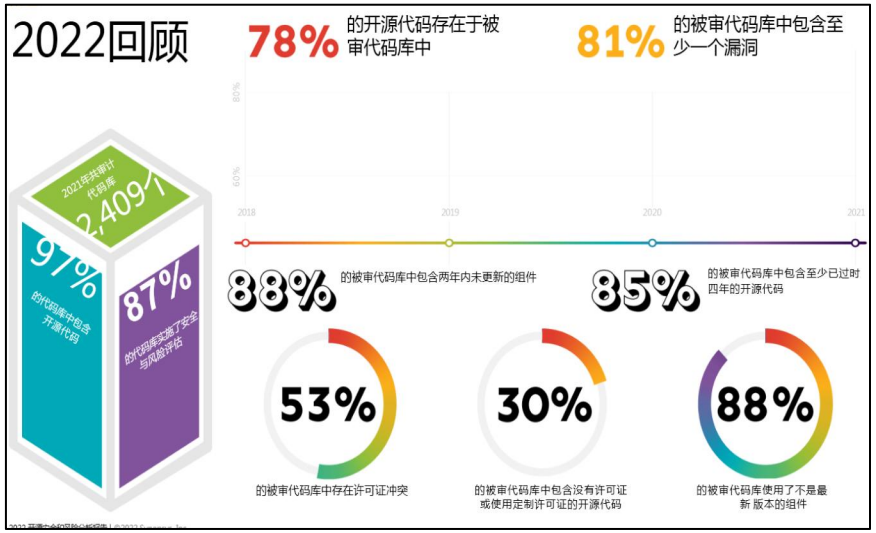
openEuler社区成立SBOM SIG决策

openEuler安全委员会

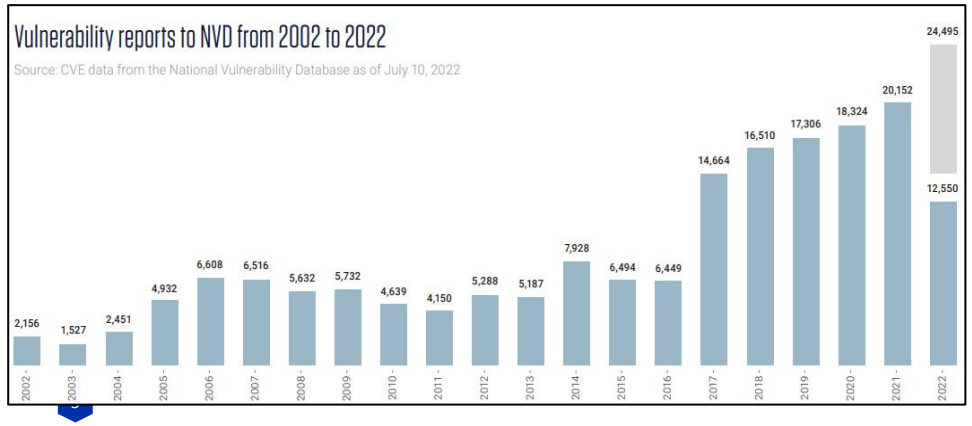
目录

开源软件行业洞察分析：使用无处不在、面临诸多不可控风险

78% 软件使用了开源，81%代码库包含至少一个漏洞
88% 2年未升级版本号，30%没有License或定制申明



NVD漏洞越来越多、CVE每月呈增长趋势、2022年增长到24495



灵魂拷问

1、如何判断我是否受影响?

在大规模软件产品中要分清楚 **我依赖了谁？ 谁依赖了我**？ 建立软件的正反向依赖关系全链路可追溯。

2、如何检测和修复软件供应链攻击?

前提是需要建立现代化的**DevSecOps软件工程体系**、从依赖分析→License分析→漏洞分析等均需要从人工排查到工程自动化。

解决方案

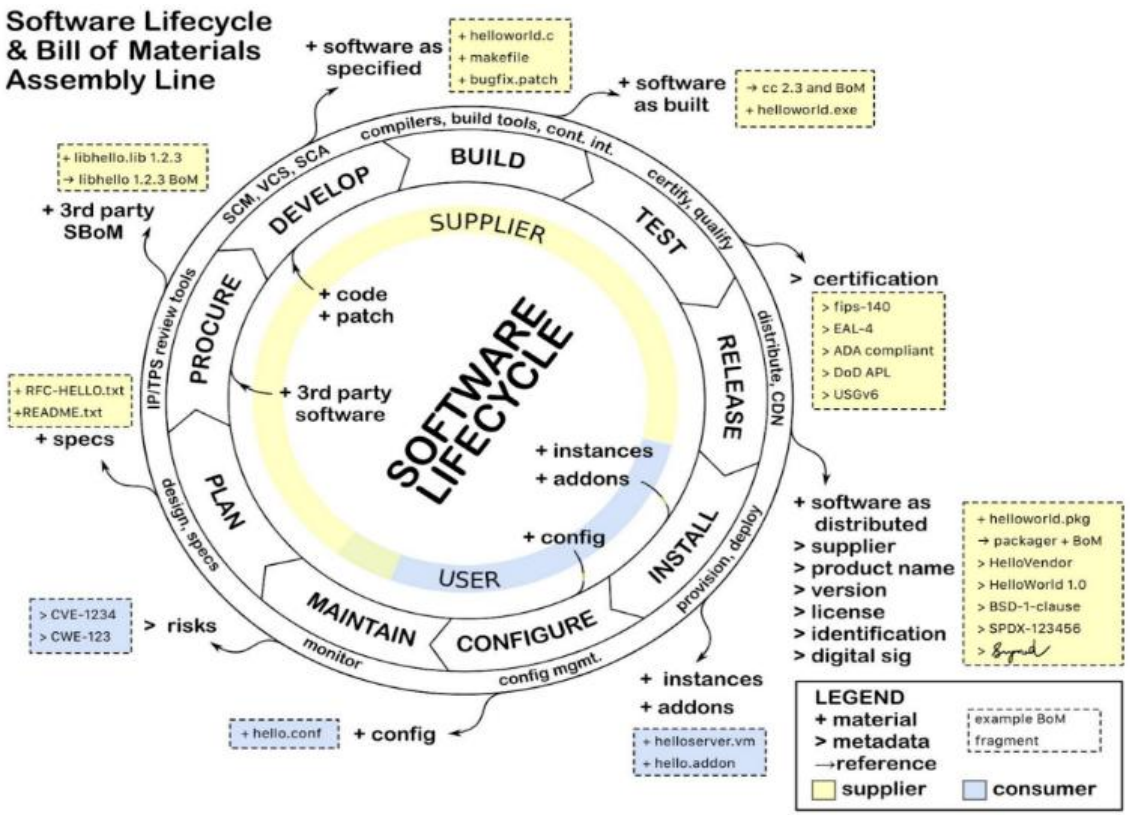
1、SBOM

2、相关配套工具

SBOM介绍：致力于软件安全供应链透明的数据底座、跨组织共享

SBOM是什么？

SBOM是一种正式标准化的、机器可读的元数据，它唯一地标识软件组件及其内容；也可能包括版权和许可证等成分数据。SBOM的宗旨是实现**跨组织共享**，有助于**提供软件供应链成分清单与透明度**。



主流SBOM数据披露标准: SPDX、CycloneDX、SWID

- **Linux Fundation**: SPDX
- **OWASP**: CycloneDX
- **ISO/IEC**: SWID 19770-2

SBOM标准	SPDX	SWID	CycloneDX
组织	Linux Fundation	ISO & IEC	OWASP
标准化	ISO/IEC 5962: Under Development	ISO/IEC 19770-2	No plan
当前版本	2.2.1	2	1.3
软件标识	Package SPDX ID, Hash	SWID	GAV, PURL, CPE, SWID, Hash
内容	Document Creation Information Package Information File Information Snippet Information Other Licensing Information Relationships Annotations	SWID Entity Payload Link rel	Meta Components Pidgrees Dependencies Compositions Vulnerabilities Signatures
工具	SPDX tools: 20	SWID tools: 12	CycloneDX Tools: 67
主要应用场景	合规场景；漏洞追溯等	软件标识：安装/发现/移除/补丁	场景分析：漏洞追溯/合规/等18种场景
转换工具	SwiftBOM, DecoderRing		

openEuler社区成立SBOM SIG的目的和价值

目的：

①孵化SBOM相关技术，形成openEuler社区统一技术路线；
②赋能伙伴，快速构建SBOM披露能力；
③参与中国SBOM披露标准建设；

价值：

对标国内外友商，围绕SBOM构建openEuler社区软件供应链安全，
打造开源合规的根社区；

国内外标准现状

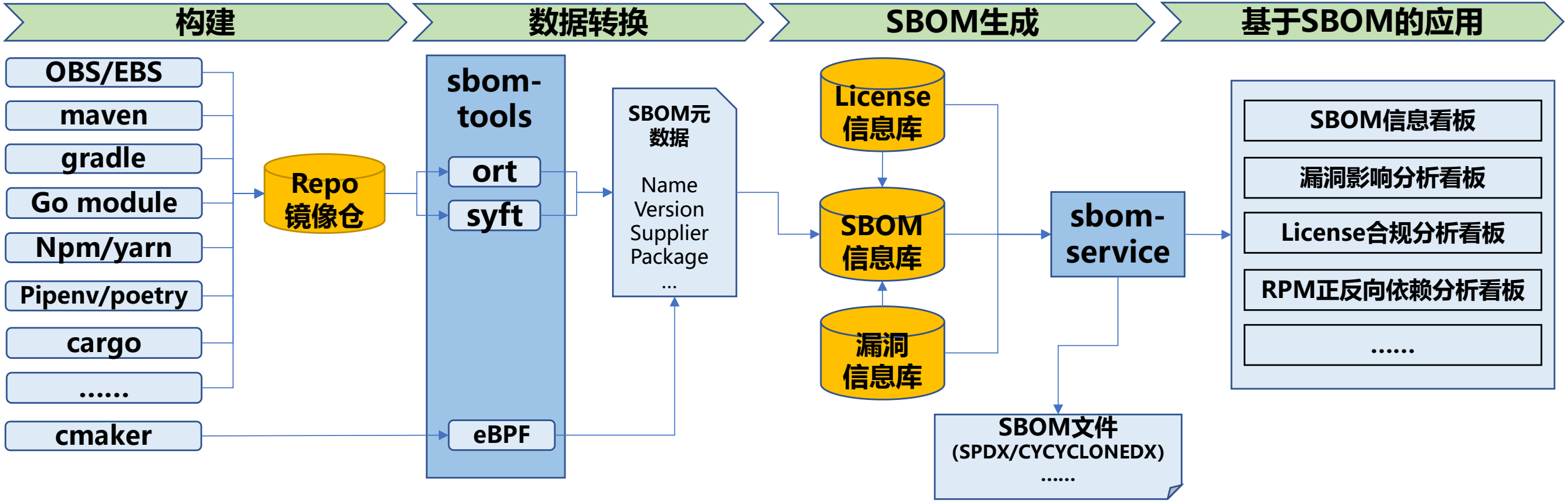
- 国内**正在推进**SBOM团标和国标的立项和制定；
- 美国国家电信和信息管理局（NTIA），2018/6/6起，启动软件组件透明度计划，定义并推动**SBOM基础格式达成行业共识**。
- 四个主要协议组织**分别发布了SBOM的披露协议**，**Linux Fundation**: SPDX，**OWASP**: CycloneDX， **ISO/IEC**: SWID 19770-2，**CISQ** & **OMG**: 3T-SBOM。
- OpenChain 在ISO 5230/18974标准中提出**软件供应链管理需要基于SBOM**。
- 欧美等多个**政府机构也在相应法规中要求提供SBOM**：

  ●**美国白宫2021年5月份发布第14028号行政令**，要求美国商务部在60天内协同(NTIA)发布软件物料清单 (SBOM) 的“最小元素”。
  ● **ENISA**：在2020/11/9发布《Guidelines For Securing The Internet Of Things》建议使用针对物联网设备的SBOM，并建议使用Dependency Track工具来管理底层软件依赖关系。
  ●荷兰**NCSC**：在2021年1月发布《Using the SBOM for Enhancing Cybersecurity》推荐基于CycloneDX，Dependency Track等整体方案。

友商分析

- **SUSE、openSUSE**：SUSE SBOM已在23年4月对外公布,23年7月提供开源SBOM生成工具。
- **RedHat**：2023年对外发布SBOM，并提供软件供应链安全E2E工具链包括SBOM生成。
- **OpenAnolis**：2023年11月起开始随ISO\RPM制品包一起，对外披露SBOM清单。
- 包括**Snyk，SonaType，Fossology**在内的众多安全软件已逐步开始支持生成SBOM或者使用SBOM作为漏洞分析的输入。

openEuler开源社区SBOM解决方案架构全景图

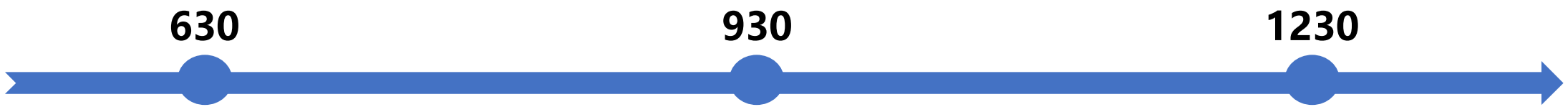


工具分类	工具名称	功能描述	openEuler Repo地址	Github Repo地址	原始工具地址
数据转换	sbom-tools	SBOM元数据获取工具	计划	https://github.com/opensourceways/sbom-tools	https://github.com/microsoft/sbom-tool
SBOM生成	sbom-service	SBOM元数据导入存库，漏洞数据，license数据集成	计划	https://github.com/opensourceways/sbom-service	https://github.com/oss-review-toolkit/ort
基于SBOM的应用服务	sbom-service	SBOM看板、漏洞信息、License信息、正反向依赖分析看板	计划	https://github.com/opensourceways/sbom-service	https://github.com/oss-review-toolkit/ort

SBOM SIG规划路标（24年规划）

目标：

①**统一**openEuler社区SBOM技术路线，建立**SBOM相关工具仓库**；
②随LTS版本发布**SPDX/CYCLONEDX**披露协议的SBOM文件；
③初步构建**基于SBOM的应用服务**，如漏洞影响分析、License合规分析和RPM正反向依赖分析；



- 支持**SPDX 2.2**格式生成；
- 支持**CYCLONEDX 1.4**格式生成；
- SBOM相关工具建仓；

- 构建基于SBOM的**应用服务**
  - 漏洞影响分析
  - License合规分析
  - RPM正反向依赖分析

- 支持**SPDX 3.0**格式生成；
- 发布**SPDX 3.0格式SBOM**文件；

openEuler社区SBOM未来能力扩展

增强RPM包构建依赖解析

- 适配支持更多的构建系统。
- 目前SBOM只有RPM直接依赖信息，缺少间接依赖信息，后续需要补齐。

支持更多SBOM披露协议

- GitBOM是用来创建简洁组件依赖关系图的工具，作为SBOM标准协议格式的补充。
- OBOM运行时环境、配置和其他依赖项的完整堆栈清单，操作信息变动时，可以与SBOM解耦，只更新OBOM信息。
- 国家SBOM协议。

增强基于SBOM的应用服务

- 加强Web服务信息管理能力，如提供CVE与ISSUE关联信息，实时更新漏洞修复状态。

SBOM SIG组成员预沟通情况

序号	企业机构	沟通情况	是否有意愿	Maintainer	Committer
1	华为	已沟通	是	√（杜泉松、罗钰凯）	√（刘政均）
2	麒麟信安	已沟通	是	√（袁佳）	√（刘星湘）
3	统信软件	已沟通	是	√（覃芝锛）	
4	超聚变	已沟通	是	√（卢棣合）	√（杨超、李恬）
5	麒麟软件	已沟通	是	√（姜昭宇）	√（张泽阳）
6	中科方德	已沟通	是	√（刘赢）	√（韩辉）

决策和建议

- 同意openEuler社区建立SBOM SIG，具体工作在安全委员会汇报；

THANKS

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler