
GOTC 2023
全球开源技术峰会
THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE
OPEN SOURCE, INTO THE FUTURE
「聚焦开源安全」专场
本期议题：用SBOM提升软件供应链安全
龙文选 2023年05月28日

议题

一、SBOM是什么

二、SBOM历史

三、软件供应链安全

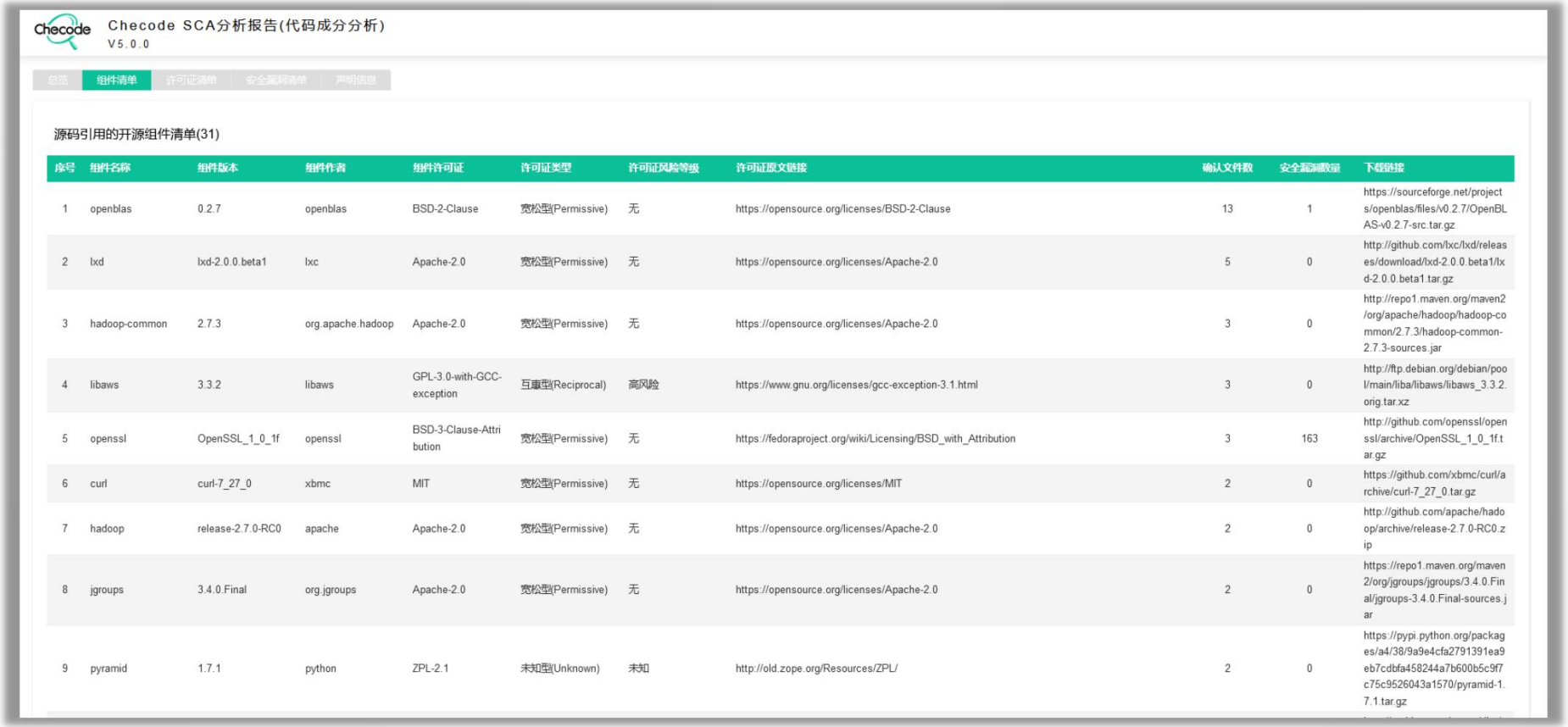
四、SBOM的作用

五、SBOM技术

六、SBOM趋势

SBOM 软件材料清单

SBOM全称是“Software Bill Of Materials” 的缩写，中文叫“软件材料清单”， 是以数据格式来描述产品结构的文件， 是一份列出生产和制造产品所需原材料的清单。



Checode SCA分析报告(代码成分分析)
V5.0.0

总览 | 组件清单 | 许可证清单 | 安全漏洞清单 | 声明信息

源码引用的开源组件清单(31)

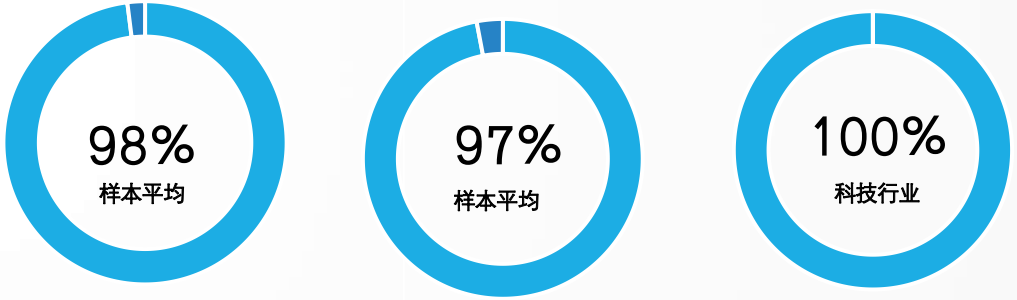
序号	组件名称	组件版本	组件作者	组件许可证	许可证类型	许可证风险等级	许可证原文链接	确认文件数	安全漏洞数量	下载链接
1	openblas	0.2.7	openblas	BSD-2-Clause	宽松型(Permissive)	无	https://opensource.org/licenses/BSD-2-Clause	13	1	https://sourceforge.net/projects/openblas/files/v0.2.7/OpenBLAS-v0.2.7-src.tar.gz
2	lxd	lxd-2.0.0.beta1	lxc	Apache-2.0	宽松型(Permissive)	无	https://opensource.org/licenses/Apache-2.0	5	0	http://github.com/lxc/lxd/releases/download/lxd-2.0.0.beta1/lxd-2.0.0.beta1.tar.gz
3	hadoop-common	2.7.3	org.apache.hadoop	Apache-2.0	宽松型(Permissive)	无	https://opensource.org/licenses/Apache-2.0	3	0	http://repo1.maven.org/maven2/org/apache/hadoop/hadoop-common/2.7.3/hadoop-common-2.7.3-sources.jar
4	libaws	3.3.2	libaws	GPL-3.0-with-GCC-exception	互惠型(Reciprocal)	高风险	https://www.gnu.org/licenses/gcc-exception-3.1.html	3	0	http://ftp.debian.org/debian/pool/main/liba/libaws/libaws_3.3.2.orig.tar.xz
5	openssl	OpenSSL_1_0_1f	openssl	BSD-3-Clause-Attribution	宽松型(Permissive)	无	https://fedoraproject.org/wiki/Licensing/BSD_with_Attribution	3	163	http://github.com/openssl/openssl/archive/OpenSSL_1_0_1f.tar.gz
6	curl	curl-7_27_0	xbmc	MIT	宽松型(Permissive)	无	https://opensource.org/licenses/MIT	2	0	https://github.com/xbmc/curl/archive/curl-7_27_0.tar.gz
7	hadoop	release-2.7.0-RC0	apache	Apache-2.0	宽松型(Permissive)	无	https://opensource.org/licenses/Apache-2.0	2	0	http://github.com/apache/hadoop/archive/release-2.7.0-RC0.zip
8	jgroups	3.4.0.Final	org.jgroups	Apache-2.0	宽松型(Permissive)	无	https://opensource.org/licenses/Apache-2.0	2	0	https://repo1.maven.org/maven2/org/jgroups/jgroups/3.4.0.Final/jgroups-3.4.0.Final-sources.jar
9	pyramid	1.7.1	python	ZPL-2.1	未知型(Unknown)	未知	http://old.zope.org/Resources/ZPL/	2	0	https://pypi.python.org/packages/a4/38/9a9e4cfa2791391ea9eb7cdbfa458244a7b600b5c9f7c75c9526043a1570/pyramid-1.7.1.tar.gz

软件吞噬世界，开源吞噬软件

开源软件助力软件开发

多　快　好　省

开源软件使用率



《软件成分清单和数字安全准备》

《2022开源安全与风险分析报告》

- 2022年9月，美国参议院国土安全和政府事务委员会投票通过了《保护开源软件法案》，该法案“**首次把开源软件认定为公共基础设施**”，提案发起人彼得斯表示：“**开源软件是数字世界的基石**”
- 2021年3月，由中国科学院软件研究所牵头承担的“开源软件供应链重大基础设施建设”项目启动。
- 2022年1月，国务院发布《 “十四五”数字经济发展规划》，指出：“**数字经济是继农业经济、工业经济之后的主要经济形态**”

SBOM由来

GOTC

- 启动GNU计划（1984）
- 创造了著佐权（Copyleft）
- 共同创造GPL许可证，

- （1985年），**创立**

FREE SOFTWARE FOUNDATION

- **发布了Linux操作系统内核并采用GPL（1993）**

- 维护Linux内核至今（1993-）
- 为Linux代码开发了GIT（2005）

THE LINUX FOUNDATION

LF AI & DATA

OpenSSF OPEN SOURCE SECURITY FOUNDATION

CHIPS ALLIANCE

CLOUD NATIVE COMPUTING FOUNDATION

- **定义开源软件，扩展了“开源软件”的概念**

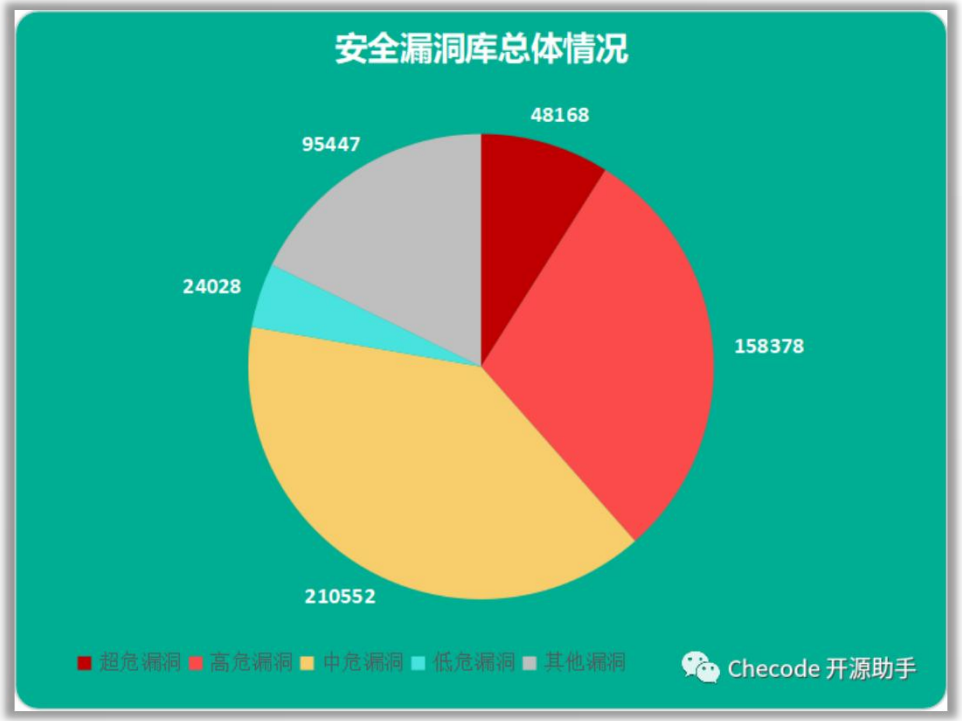
- 批准了共九类数十个许可证，被广泛接受和采用
- 鼓励更为宽松的开源软件，接纳对企业用户友好的许可证

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

开源软件漏洞危害大

安全漏洞库总体情况



奇科厚德从 CNNVD、 CNVD、NVD 收集全球软件漏洞信息，并持续为用户提供漏洞库更新服务和预警服务。截止2023年5月5日，奇科厚德信息安全漏洞库收集漏洞53万+。其中高危漏洞、超危漏洞占比38.5%

影响全球的超危开源漏洞

HeartBleed漏洞 2014年

- OpenSSL开源组件超危漏洞
- Heartbleed能让攻击者从服务器内存中读取包括用户名、密码和信用卡号等隐私信息在内的数据，已经波及大量互联网公司
- 受影响的服务器数量可能多达几十万。其中已被确认受影响的网站包括Imgur、OKCupid、Eventbrite 以及 FBI 网站等

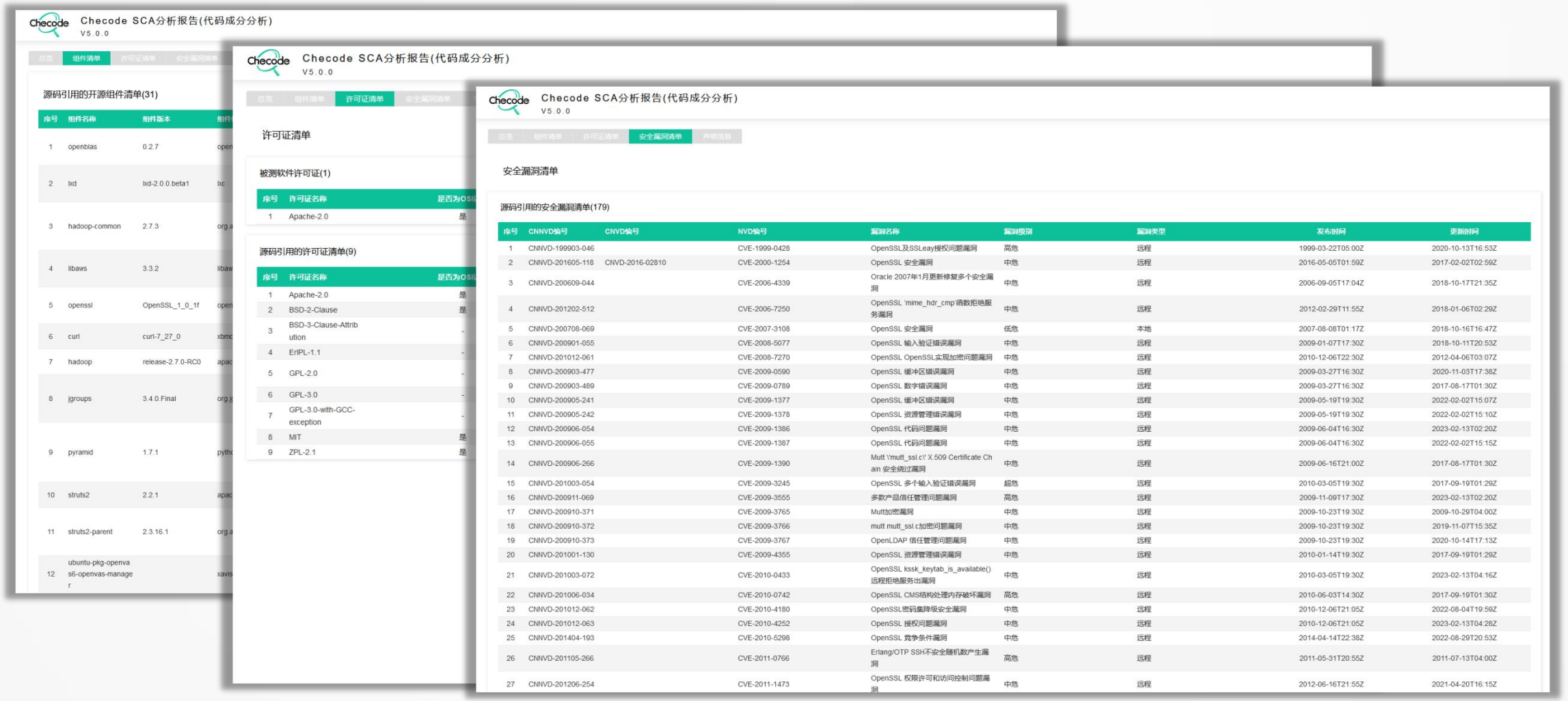
Log4J2 漏洞 2021年

- Apache Log4j2开源组件安全的高危漏洞
- 攻击者仅需一段代码就可远程控制受害者服务器，不需要用户执行任何多余操作即可触发该漏洞，使攻击者可以远程控制用户受害者服务器，90%以上基于java开发的应用平台都会受到影响。
- 今后十年甚至更长时间，该漏洞的影响仍然可能存在

开源治理推动SBOM方法论和技术演进

	第一阶段 1995年-2005年	第二阶段 2005年-2015年	第三阶段 2015年-
方法论	开源合规	开源安全及合规	软件供应链安全
代码引入	代码静态分析 代码特征扫描	代码特征扫描 组件漏洞分析	代码特征扫描 组件漏洞分析
组件引入	Web组件生态形成和繁荣阶段		依赖关系扫描 二进制扫描

SBOM检测工具的结果



Checode SCA分析报告(代码成分分析)
V5.0.0

总览 | 组件清单 | 许可证清单 | 安全漏洞清单

源码引用的开源组件清单(31)

序号	组件名称	组件版本
1	openblas	0.2.7
2	lxd	lxd-2.0.0.beta1
3	hadoop-common	2.7.3
4	libaws	3.3.2
5	openssl	OpenSSL_1_0_1f
6	curl	curl-7_27_0
7	hadoop	release-2.7.0-RC0
8	jgroups	3.4.0.Final
9	pyramid	1.7.1
10	struts2	2.2.1
11	struts2-parent	2.3.16.1
12	ubuntu-pkg-openvas6-openvas-manager	

Checode SCA分析报告(代码成分分析)
V5.0.0

总览 | 组件清单 | 许可证清单 | 安全漏洞清单

许可证清单

被测软件许可证(1)

序号	许可证名称	是否为OSI
1	Apache-2.0	是

源码引用的许可证清单(9)

序号	许可证名称	是否为OSI
1	Apache-2.0	是
2	BSD-2-Clause	是
3	BSD-3-Clause-Attribution	-
4	ErlPL-1.1	-
5	GPL-2.0	-
6	GPL-3.0	-
7	GPL-3.0-with-GCC-exception	-
8	MIT	是
9	ZPL-2.1	是

Checode SCA分析报告(代码成分分析)
V5.0.0

总览 | 组件清单 | 许可证清单 | 安全漏洞清单 | 声明信息

安全漏洞清单

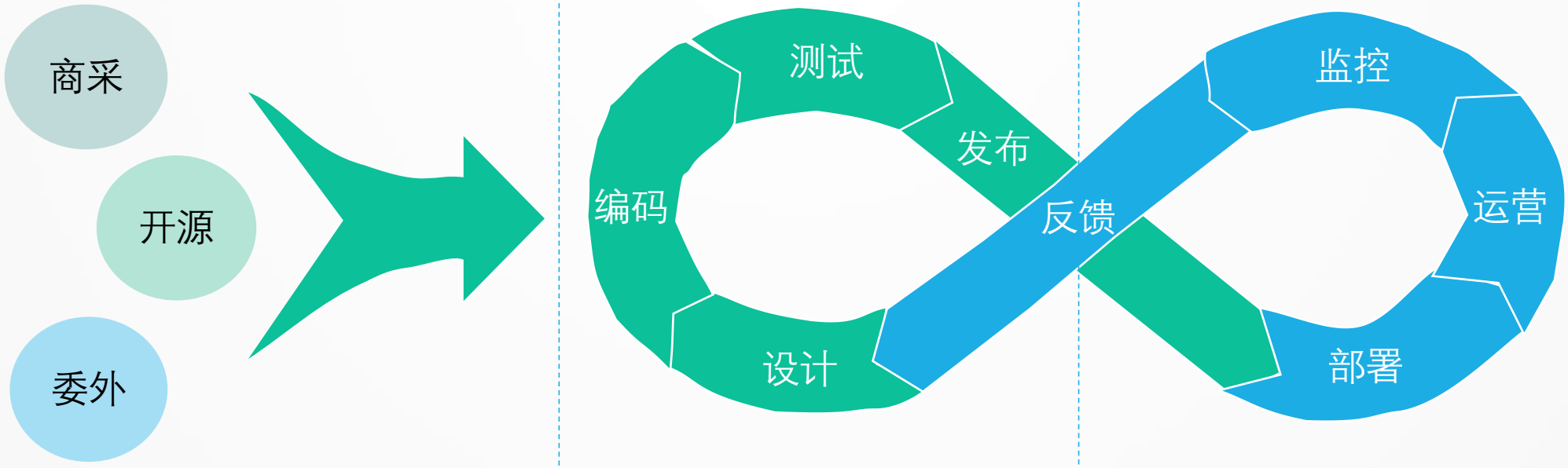
源码引用的安全漏洞清单(179)

序号	CNNVD编号	CNVD编号	NVD编号	漏洞名称	漏洞级别	漏洞类型	发布时间	更新时间
1	CNNVD-199903-046		CVE-1999-0428	OpenSSL及SSLeay授权问题漏洞	高危	远程	1999-03-22T05:00Z	2020-10-13T16:53Z
2	CNNVD-201605-118	CNVD-2016-02810	CVE-2000-1254	OpenSSL 安全漏洞	中危	远程	2016-05-05T01:59Z	2017-02-02T02:59Z
3	CNNVD-200609-044		CVE-2006-4339	Oracle 2007年1月更新修复多个安全漏洞	中危	远程	2006-09-05T17:04Z	2018-10-17T21:35Z
4	CNNVD-201202-512		CVE-2006-7250	OpenSSL 'mime_hdr_cmp'函数拒绝服务漏洞	中危	远程	2012-02-29T11:55Z	2018-01-06T02:29Z
5	CNNVD-200708-069		CVE-2007-3108	OpenSSL 安全漏洞	低危	本地	2007-08-08T01:17Z	2018-10-16T16:47Z
6	CNNVD-200901-055		CVE-2008-5077	OpenSSL 输入验证错误漏洞	中危	远程	2009-01-07T17:30Z	2018-10-11T20:53Z
7	CNNVD-201012-061		CVE-2008-7270	OpenSSL OpenSSL实现加密问题漏洞	中危	远程	2010-12-06T22:30Z	2012-04-06T03:07Z
8	CNNVD-200903-477		CVE-2009-0590	OpenSSL 缓冲区错误漏洞	中危	远程	2009-03-27T16:30Z	2020-11-03T17:38Z
9	CNNVD-200903-489		CVE-2009-0789	OpenSSL 数字错误漏洞	中危	远程	2009-03-27T16:30Z	2017-08-17T01:30Z
10	CNNVD-200905-241		CVE-2009-1377	OpenSSL 缓冲区错误漏洞	中危	远程	2009-05-19T19:30Z	2022-02-02T15:07Z
11	CNNVD-200905-242		CVE-2009-1378	OpenSSL 资源管理错误漏洞	中危	远程	2009-05-19T19:30Z	2022-02-02T15:10Z
12	CNNVD-200906-054		CVE-2009-1386	OpenSSL 代码问题漏洞	中危	远程	2009-06-04T16:30Z	2023-02-13T02:20Z
13	CNNVD-200906-055		CVE-2009-1387	OpenSSL 代码问题漏洞	中危	远程	2009-06-04T16:30Z	2022-02-02T15:15Z
14	CNNVD-200906-266		CVE-2009-1390	Mutt \'mutt_ssl.c\' X.509 Certificate Chain 安全绕过漏洞	中危	远程	2009-06-16T21:00Z	2017-08-17T01:30Z
15	CNNVD-201003-054		CVE-2009-3245	OpenSSL 多个输入验证错误漏洞	超危	远程	2010-03-05T19:30Z	2017-09-19T01:29Z
16	CNNVD-200911-069		CVE-2009-3555	多款产品信任管理问题漏洞	高危	远程	2009-11-09T17:30Z	2023-02-13T02:20Z
17	CNNVD-200910-371		CVE-2009-3765	Mutt加密漏洞	中危	远程	2009-10-23T19:30Z	2009-10-29T04:00Z
18	CNNVD-200910-372		CVE-2009-3766	mutt mutt_ssl.c加密问题漏洞	中危	远程	2009-10-23T19:30Z	2019-11-07T15:35Z
19	CNNVD-200910-373		CVE-2009-3767	OpenLDAP 信任管理问题漏洞	中危	远程	2009-10-23T19:30Z	2020-10-14T17:13Z
20	CNNVD-201001-130		CVE-2009-4355	OpenSSL 资源管理错误漏洞	中危	远程	2010-01-14T19:30Z	2017-09-19T01:29Z
21	CNNVD-201003-072		CVE-2010-0433	OpenSSL kssk_keytab_is_available() 远程拒绝服务出漏洞	中危	远程	2010-03-05T19:30Z	2023-02-13T04:16Z
22	CNNVD-201006-034		CVE-2010-0742	OpenSSL CMS结构处理内存破坏漏洞	高危	远程	2010-06-03T14:30Z	2017-09-19T01:30Z
23	CNNVD-201012-062		CVE-2010-4180	OpenSSL密码集降级安全漏洞	中危	远程	2010-12-06T21:05Z	2022-08-04T19:59Z
24	CNNVD-201012-063		CVE-2010-4252	OpenSSL 授权问题漏洞	中危	远程	2010-12-06T21:05Z	2023-02-13T04:28Z
25	CNNVD-201404-193		CVE-2010-5298	OpenSSL 竞争条件漏洞	中危	远程	2014-04-14T22:38Z	2022-08-29T20:53Z
26	CNNVD-201105-266		CVE-2011-0766	Erlang/OTP SSH不安全随机数产生漏洞	高危	远程	2011-05-31T20:55Z	2011-07-13T04:00Z
27	CNNVD-201206-254		CVE-2011-1473	OpenSSL 权限许可和访问控制问题漏洞	中危	远程	2012-06-16T21:55Z	2021-04-20T16:15Z

软件供应链安全

软件供应链：

软件供应链是根据软件生命周期中一系列环节与传统供应链的相似性，由传统供应链概念扩展而来，指一个通过一级或多级软件设计、开发阶段编写软件，并通过软件交付渠道将软件从软件供应商侧送往软件用户侧的结构。



国际软件供应链安全和SBOM相关法规和标准

2021年5月
关于改善国家网络安全的总统行政命令（EO 14028）

2021年2月
第14017 号《美国供应链行政令》

2018年12月
《联邦采购供应链安全法案》

2022年9月，
欧盟发布《网络弹性法案》

2021年7月
欧洲网络与信息安全局（ENISA）发布《供应链攻击威胁情景》报告

2015年8月
欧洲网络与信息安全局发布《供应链完整性：ICT 供应链风险和挑战概述及发展方向愿景》报告

ISO/IEC 27036《信息技术安全技术供应商关系的信息安全》系列标准
ISO/IEC 20243《信息技术开放可信技术提供商标准减少恶意和仿冒组件》系列标准
ISO 28000　《供应链安全管理体系规范》

SBOM标准

2021年7月，美国商务部NTIA根据EO 14028要求发布了《软件物料清单（SBOM）的最小元素》

基线组件信息

- SBOM发布者名称
- 软件供应商名称
- 组件名称
- 组件版本
- 组件哈希
- 唯一标识号
- 组件关系

自动化支持

标准	文件位置	说明
SPDX	https://spdx.github.io/spdx-spec/	源于合规性要求，源码引用为主
CycloneDX	https://cyclonedx.org/	源于安全漏洞追踪，能记录漏洞的详细信息
SWID	ISO/IEC 19770-2:2015	利于追踪软件资产的全生命周期

实践和进程

- 发布频率
- 信息深度
- 已知的未知
- 分发和交付
- 访问控制
- 容错空间

我国的软件供应链安全和SBOM相关法规和标准

GOTC

法规

《“十四五”数字经济发展规划》指出：“数字经济是继农业经济、工业经济之后的主要经济形态，…实施产业链强链补链行动，加强面向多元化应用场景的技术融合和产品创新，提升产业链关键环节竞争力，完善5G、集成电路、新能源汽车、人工智能、工业互联网等重点产业供应链体系。”

《网络安全审查办法》：为了确保关键信息基础设施供应链安全，维护国家安全，对关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应进行网络安全审查。

《网络安全法》：分别从网络安全审查、网络产品和服务安全角度对供应链安全提出要求。

标准

GB/T 32921–2016《信息安全技术 信息技术产品供应方行为安全准则》

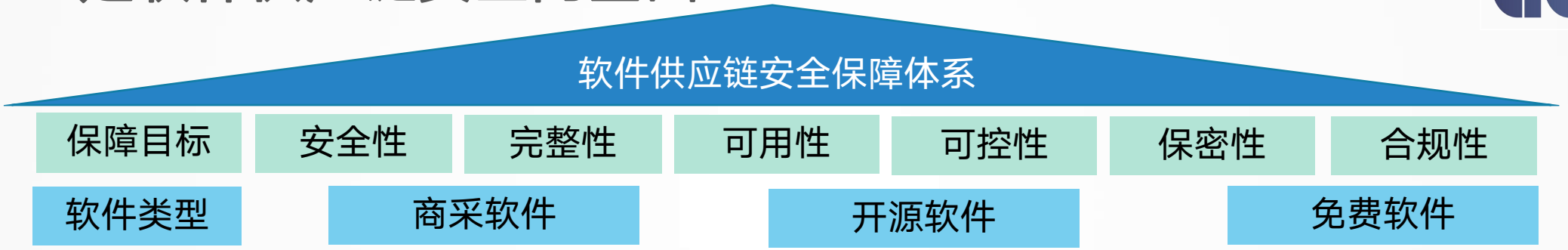
GB/T 29245–2012《信息安全技术 政府部门信息安全管理基本要求》

GB/T 36637–2018《信息安全技术 ICT供应链安全风险管理指南》

2022年6月，中国信通院《软件物料清单实践指南》

2022年6月，建信金科与中国信通院联合《软件物料清单(SBOM)安全应用白皮书》

SBOM是软件供应链安全的基础



引入环节	
软件来源	供应商资质
	开源社区活跃度
软件安全合规	软件物料清单
	软件安全要求
	软件合规要求
	安全测试机评审报告
	安全监控防护
软件资产	供应链清单管理
	版本管理
	漏洞管理
服务支持	产品及用户文档
	服务水平协议
	信息安全服务协议
安全应急响应	应急预案
	应急响应团队

生产环节	
产品设计	组件选择
编码	组件使用
	版本管理
	编程规范
	文档管理
构建	供应链清单管理
	版本管理
测试	功能/性能测试
	软件成分分析
	静态应用安全测试
	动态应用安全测试
	渗透测试
发布	产品和用户文档
	软件成分清单

使用环节	
软件来源	供应商资质
软件安全合规	软件物料清单
	软件安全要求
	软件合规要求
	安全测试机评审报告
	安全监控防护
软件资产	供应链清单管理
	版本管理
	漏洞管理
服务支持	产品及用户文档
	服务水平协议
	信息安全服务协议
安全应急响应	应急预案
	应急响应团队

采用SBOM的优势

政府视角

增加软件供应链透明性
实现软件供应链的管控
降低解决风险问题的难度
提升国家信息安全水平

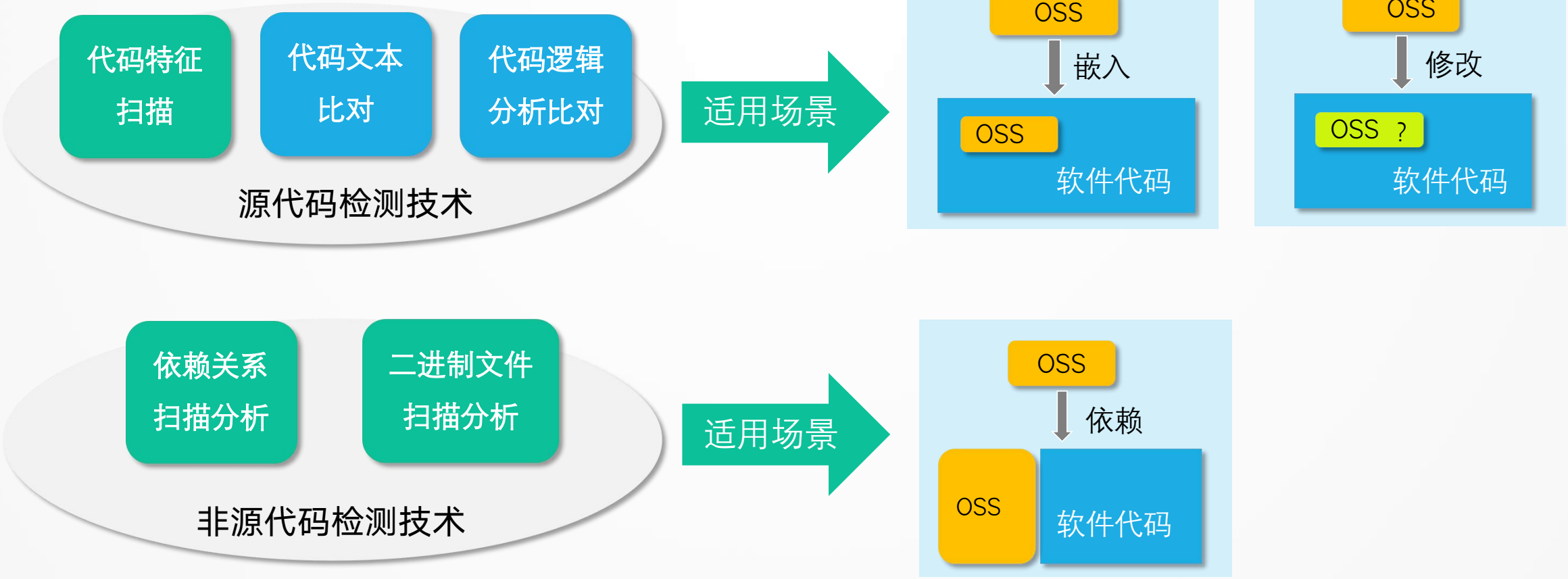
供应商视角

满足政府监管要求
响应用户的要求
加快解决安全问题速度
提升产品的竞争力
更好地支持合规和报告

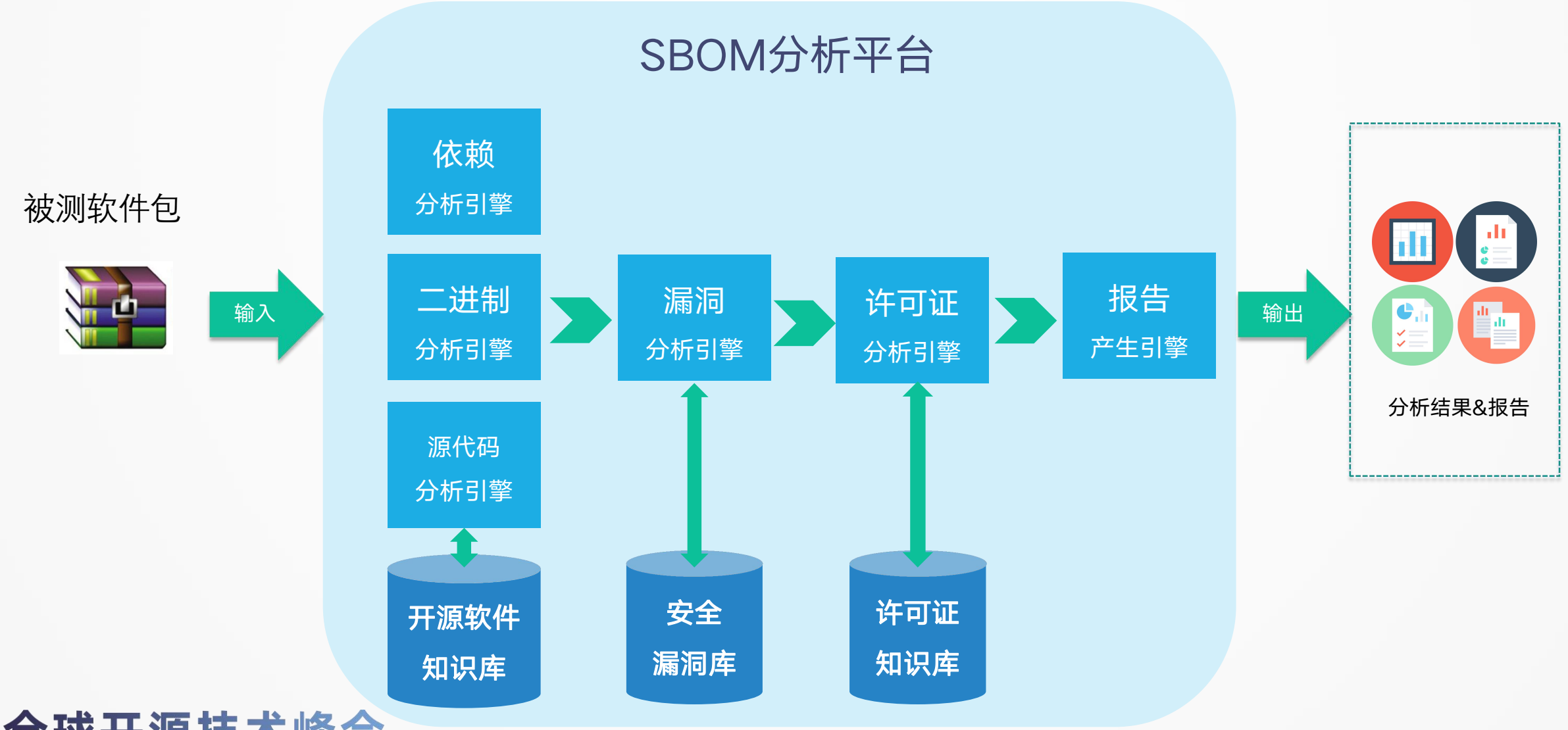
用户视角

满足监管要求
降低解决安全问题的难度
加快解决安全问题的速度
减少风险和损失
开源治理的必要手段

构造SBOM的技术


代码特征扫描
代码文本比对
代码逻辑分析比对
源代码检测技术
适用场景
OSS
嵌入
OSS
软件代码
OSS
修改
OSS ?
软件代码
依赖关系扫描分析
二进制文件扫描分析
非源代码检测技术
适用场景
OSS
依赖
OSS
软件代码

构造SBOM的流程


被测软件包
输入
SBOM分析平台
依赖
分析引擎
二进制
分析引擎
源代码
分析引擎
开源软件
知识库
漏洞
分析引擎
安全
漏洞库
许可证
分析引擎
许可证
知识库
报告
产生引擎
输出
分析结果&报告

SBOM趋势

标准化

形成有中国特色的SBOM标准体系，服务于开源社区、数字经济、信创产业

服务差异化

行业特色明显，进一步提升服务价值

集成化

与DevOps集成，融合更多安全情报，提供快速响应能力

云服务化

充分利用大数据AI能力，构造新型SBOM平台；为企业、行业、社区提供基于SaaS服务的SBOM分析、存储服务

GOTC

THANKS

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE