开源社
kaiyuanshe

SBOM驱动软件供应链安全建设最佳实践

朱贤曼　上海安势信息技术有限公司
产品架构总监

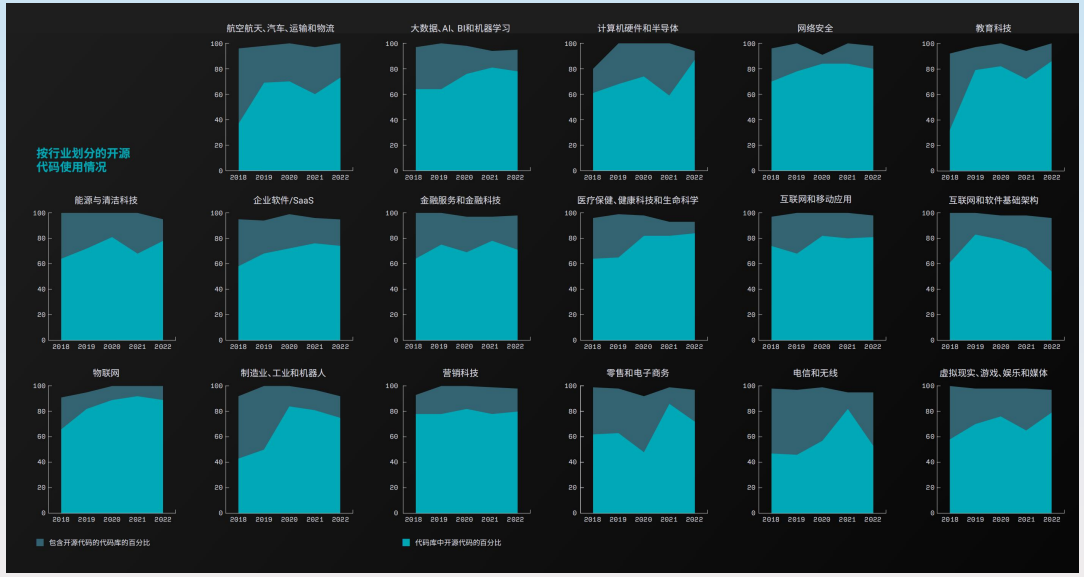
目录

CONTENTS

开源社 kaiyuanshe

01 开源洞察：机遇与挑战并存

开源洞察-机遇



据OSSRA《2023年开源安全和风险分析报告》，在调研的近20个行业中

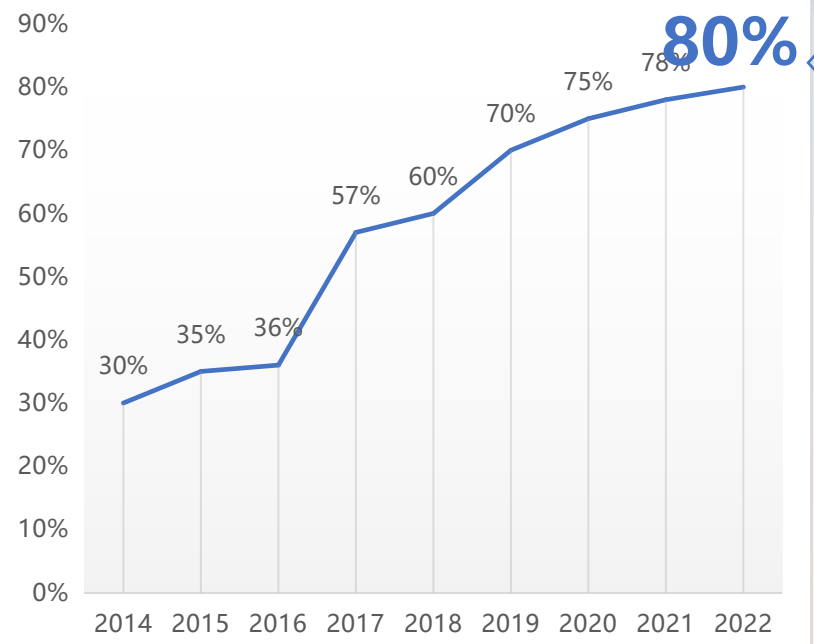
- 2022年，除电信、互联网&软件基础架构行业外，其余行业开源代码在代码库中的占比均超70%；
- 2018-2022年，所有的行业的开源代码比重基本呈现增长趋势，其中教育科技行业的开源代码占比增长了163%；航空航天、汽车、运输和物流行业增长了97%；制造业和机器人行业增长了74%；

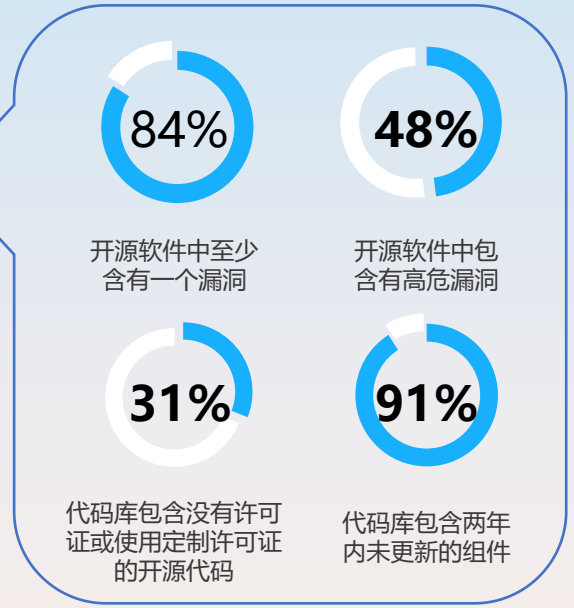
- 节省开发成本
- 开源提升代码质量
- 提高代码的可靠性
- 增加软件透明度
- 促进软件创新发展

开源洞察-挑战

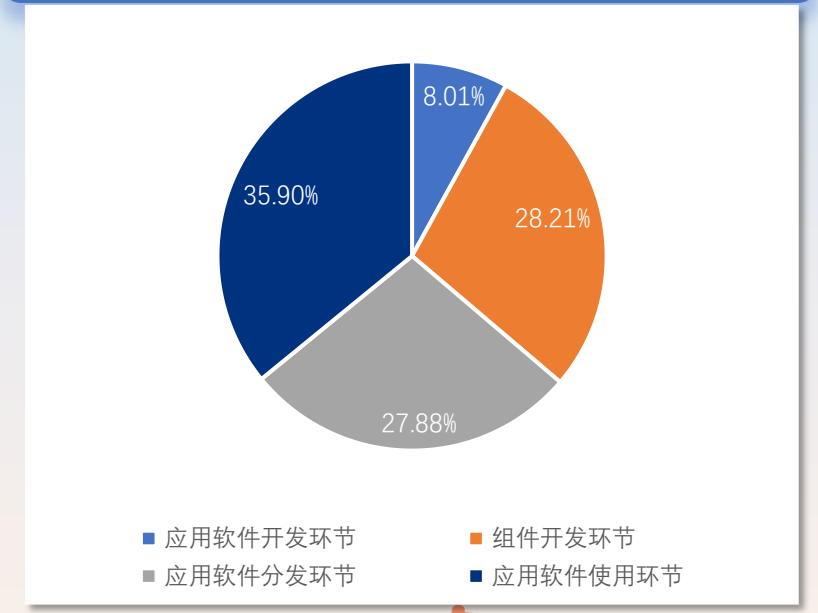
开源社 kaiyuanshe

从2014年-2022年开源代码在软件代码中的占比





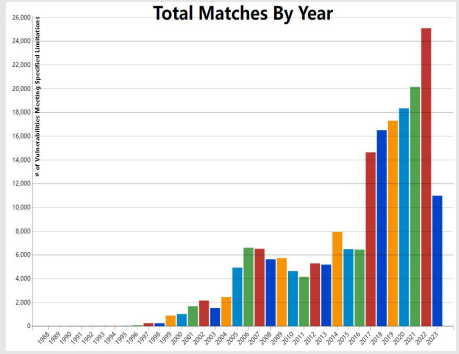
软件供应链各个环节出现的攻击事件占比



开源洞察-开源风险

供应链安全事件呈增长趋势

据权威统计，具有较高影响力的软件供应链攻击和泄露事件呈现逐年递增趋势；NVD收录的漏洞也逐年递增。



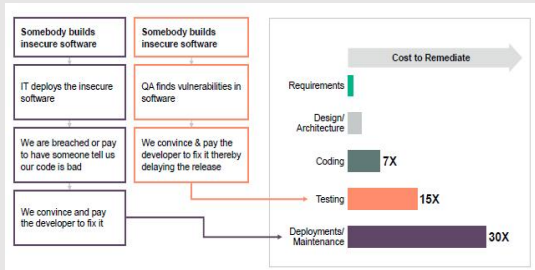
国内外许可证违规案例层出不穷

- 2008-12：FSF诉思科违反GPL协议，庭外和解，捐赠大笔资金；
- 2021-06：罗盒诉风灵违规使用GPL组件，风灵停止侵权并赔偿50万；
- 2021-10：SFC 起诉北美电视厂商 Vizio 违法GPL协议，要求其履行在Copyleft合规性要求下的义务，Vizio败诉；
- 2023-5：赤兔违规引用了Apache项目代码，修改包名并删除文件头的版权和许可证信息，遭社区谴责。

后期发现修复&整改成本高

修复&整改成本最高的阶段是在软件上线后和正在使用时。

DevSecOps的开发模式，安全左移，将安全融入整个研发流程，可以有效避免后期发现的修复成本高的问题。



02 SBOM——
缓解软件供应链风险的关键

SBOM作用

软件物料清单SBOM是一个全面的、结构化的清单，列举出了软件产品或应用程序中所使用的全部组件、库以及依赖项，具体内容包括每个组件的名称、版本以及许可证等详细信息。主流SBOM标准包括SPDX、CycloneDX、SWID等。

提高软件供应链透明度

方便跨组织共享和交换数据

高效快速地进行供应链风险管理

统一输出格式，方便建立生态

SBOM使用现状

越来越多的企业打算将其整合到DevOps流程和合规流程中

据Linux基金会发布的《软件物料清单和网络安全准备读现状》报告称：

- 2023年使用SBOM的组织：**88%**
- 主动参与解决SBOM的组织：**76%**
- 正在使用SBOM的组织：**47%**

在使用SBOM的组织及相关人士表示使用SBOM的好处主要体现在：

- **51%**的人认为：生成SBOM有助于开发人员理解应用程序中各**组件之间的依赖关系**
- **49%**的人认为：SBOM使得**监控组件漏洞**变得更加容易
- **44%**的人认为：生成SBOM有助于**开源软件许可证的合规性管理**

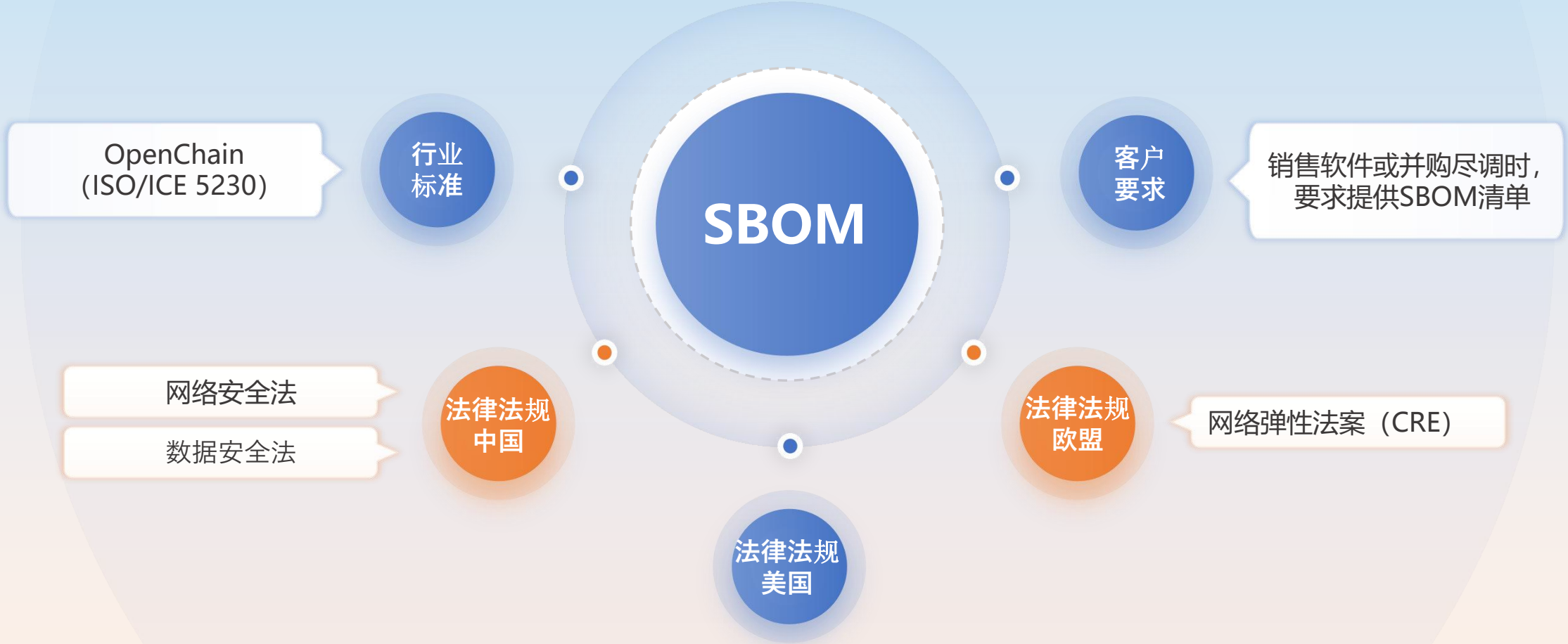
使用SBOM：

53%的人认为：SBOM有助于**预警和遵守合规性**

53%的人认为：SBOM有助于**基于风险的最终决策**

49%的人认为：SBOM中的漏洞报告有助于组织**更快的理解安全风险**

建立SBOM的必要性（政策导向）



谁需要SBOM—SBOM对各方的好处

SBOM对各方的好处

软件生产者

使用SBOM来协助构建和维护其提供的软件

- **安全**：软件生产者使用 SBOM 来确保组件是最新的版本并可以对新出现漏洞做出快速响应
- **合规**：SBOM 可以帮助生产商了解需要遵循的许可义务

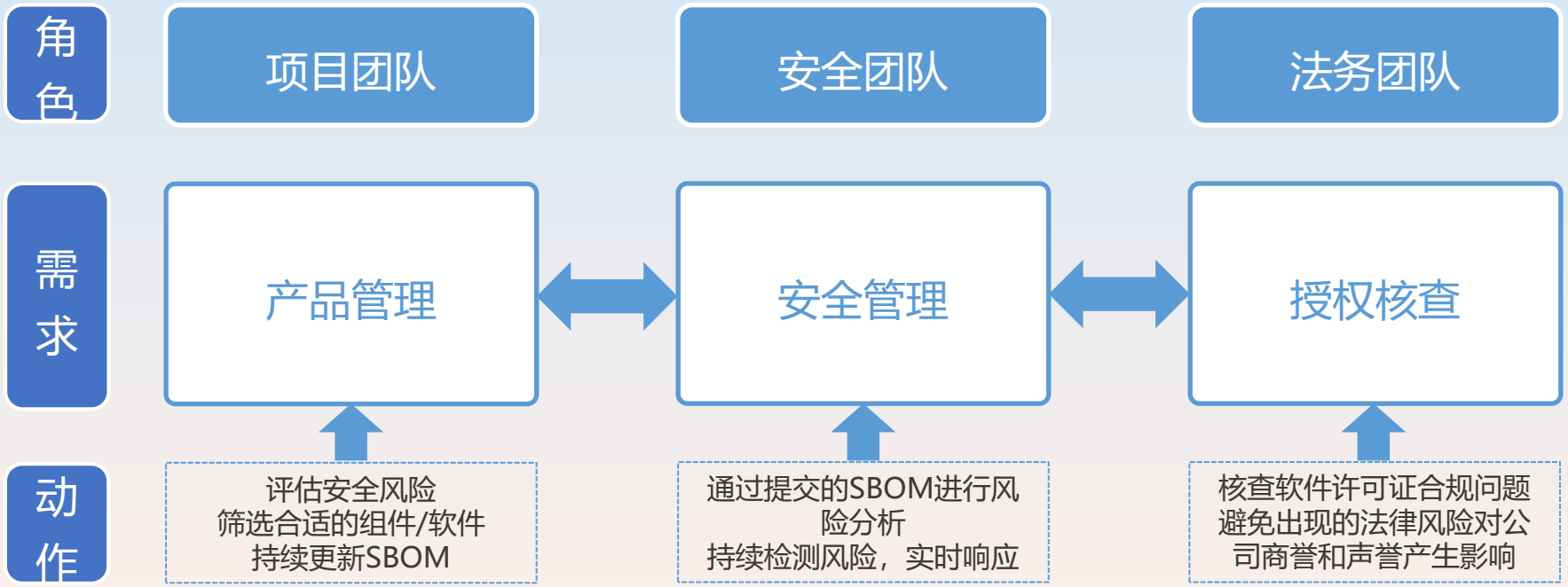
有助于提升开发效率和有效性，最终提升管理效能

软件使用者

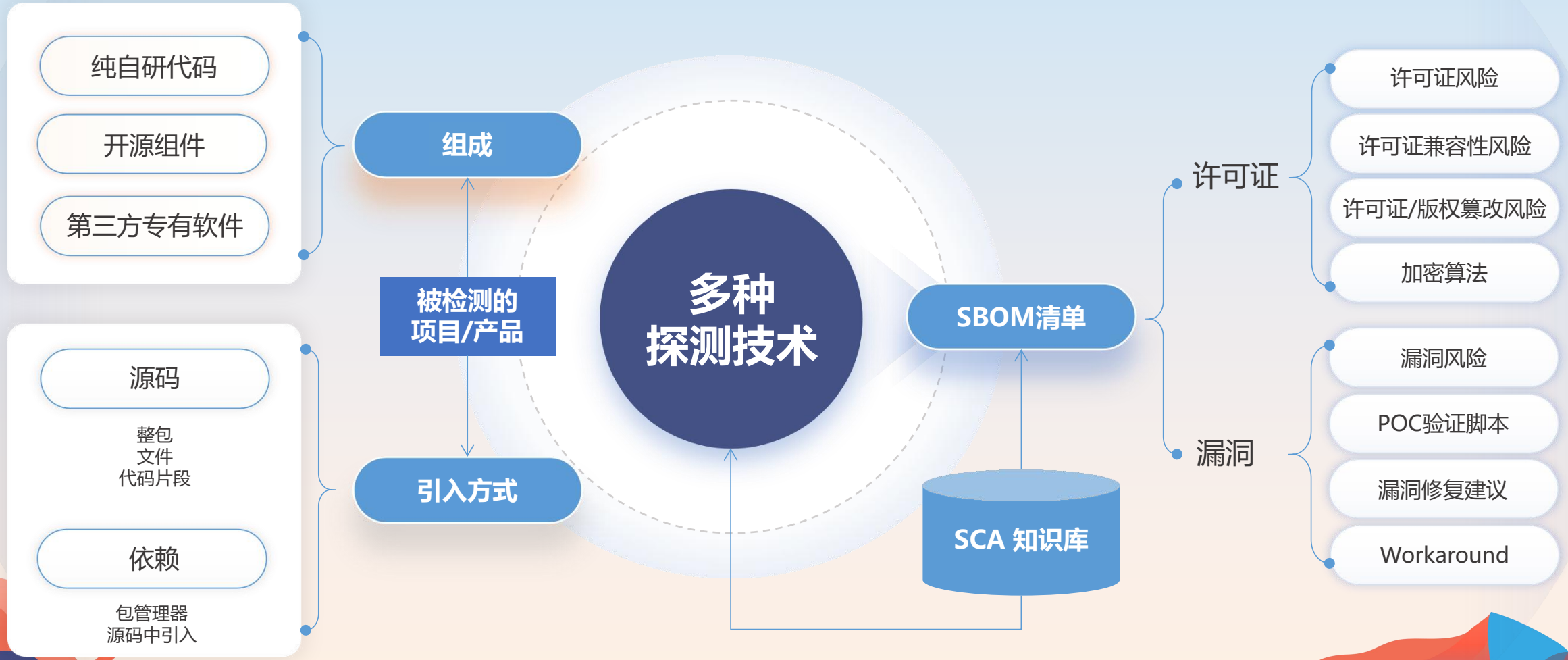
使用SBOM可以增强其漏洞风险管理能力

- 依赖 SBOM 提供的软件生态系统间的依赖信息，软件使用者可以更快速准确地识别和评估新发现漏洞的相关风险，提升响应速度，最终提升风险管理能力

谁需要SBOM—企业不同角色

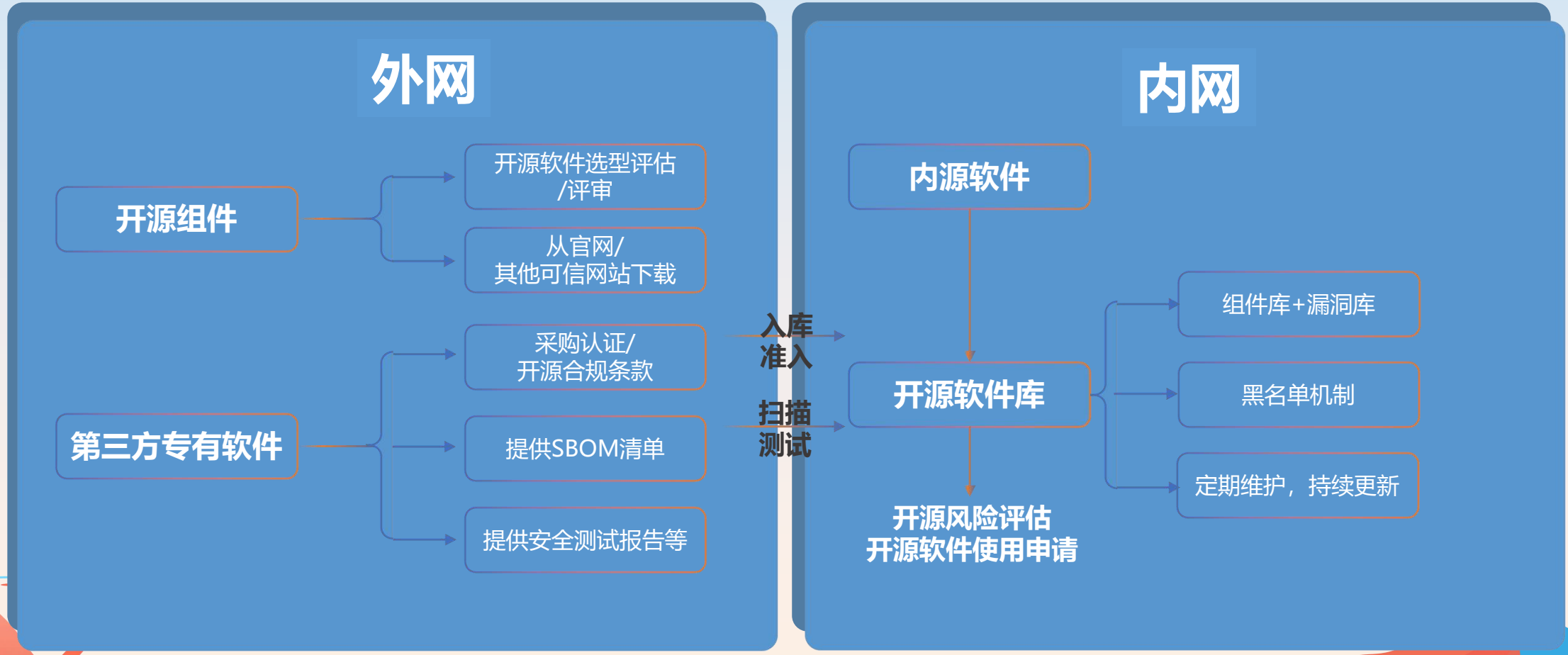


SBOM梳理面临巨大的挑战，需要借助专业SCA工具



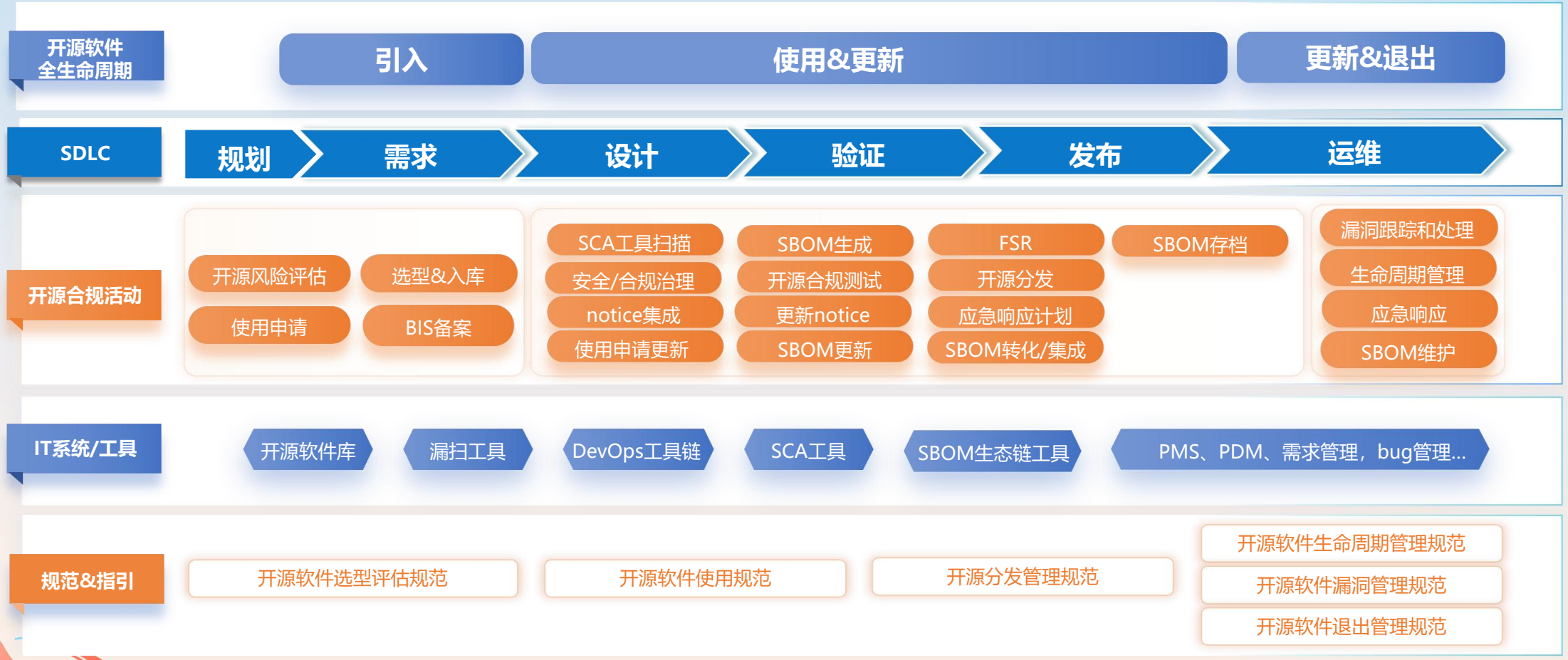
风险防范—让可靠合适的组件进入到SBOM

安全左移，建立准入机制，自建开源软件库管理开源、第三方专有及自研组件



将开源治理融入到企业现有的SDLC流程中

开源治理是个系统工程，涉及组织、流程、工程、技术和工具链等各方面，其中SBOM的生成、更新、转换、集成和存档贯穿整个SDLC



03 企业构建SBOM的展望

企业构建SBOM的展望

开源社 kaiyuanshe

1、数据字段：建立一个一致、统一的结构，用以展示和捕捉软件中组件的信息

2、自动化支持：自动化生成能力和机器可读性的提前是统一标准的数据格式

3、流程和最佳实践：实现 SBOM 的价值更多体现在 SBOM 使用机制的实践和流程上，并将其集成到安全开发生命周期的日常活动中

4、企业和组织要尽可能多的捕获整个软件生命周期的细节，并有加密做保证，以防被篡改

5、融入自动化的工具和流程的同时也需要具备消化这些自动化流程的能力

6、提高 SBOM 的人、机可读性，就需要专业的语义解读能力和数据的标准化和规范化

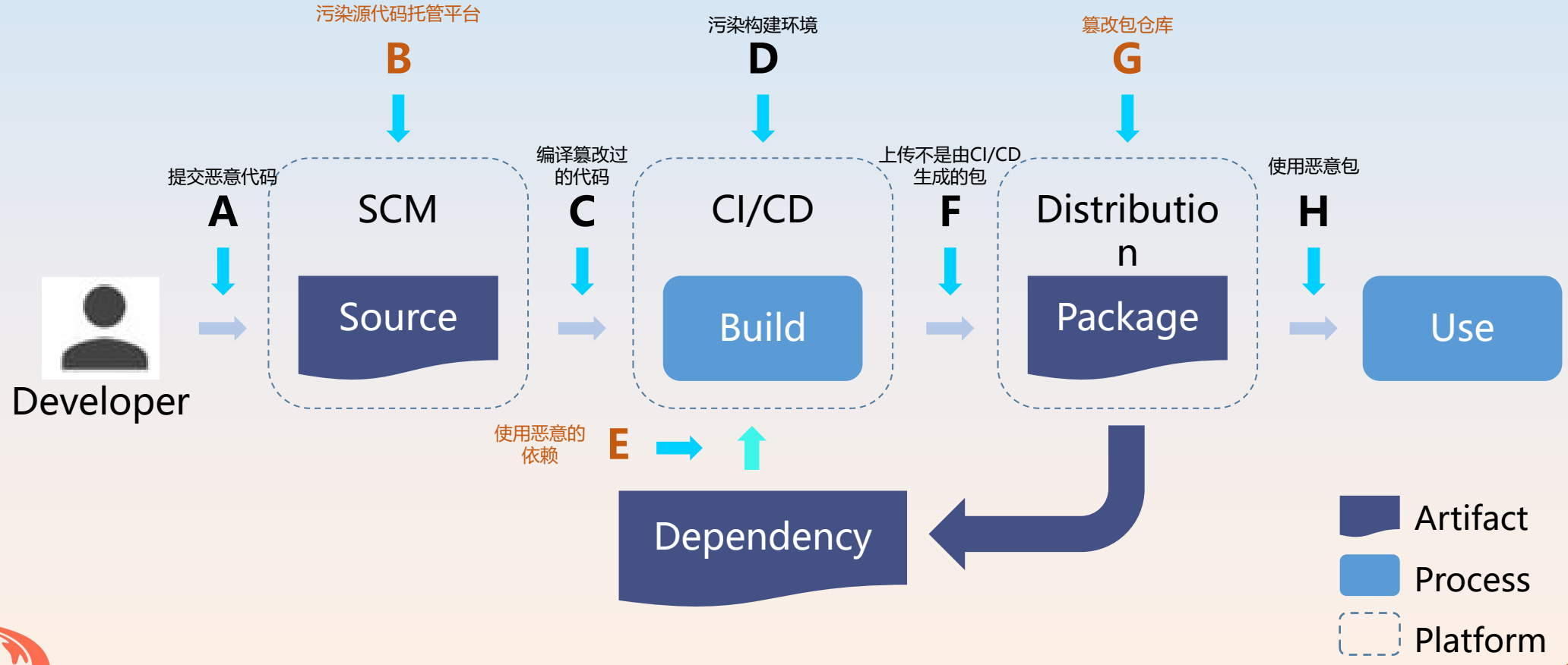
7、对于动态的依赖关系、第三方服务的调用和其他没有直接包含在软件构建中的依赖关系都需要纳入 SBOM 的范畴之中

8、SBOM 的不断创新，模块化结构可以最好地支持多样化的创新和适应性

9、SBOM 不应独立于软件领域，应与硬件数据联系起来

04 SBOM之外的解决方案

软件生产各环节均面临安全挑战，SBOM无法全覆盖



SBOM之外的解决方案

01 **构建完整性：**确保包是根据软件生产者定义的构建方式从正确的未修改的源和依赖项构建而来，且制品在开发各阶段传递时不被篡改

- ✓ 在构建服务器用脚本构建，且对构建脚本进行版本控制
- ✓ 构建环境：临时、相互隔离、不联网
- ✓ 无构建参数，构建所涉及的依赖、源和构建步骤都是事先定义好的且有着不可变的引用地址

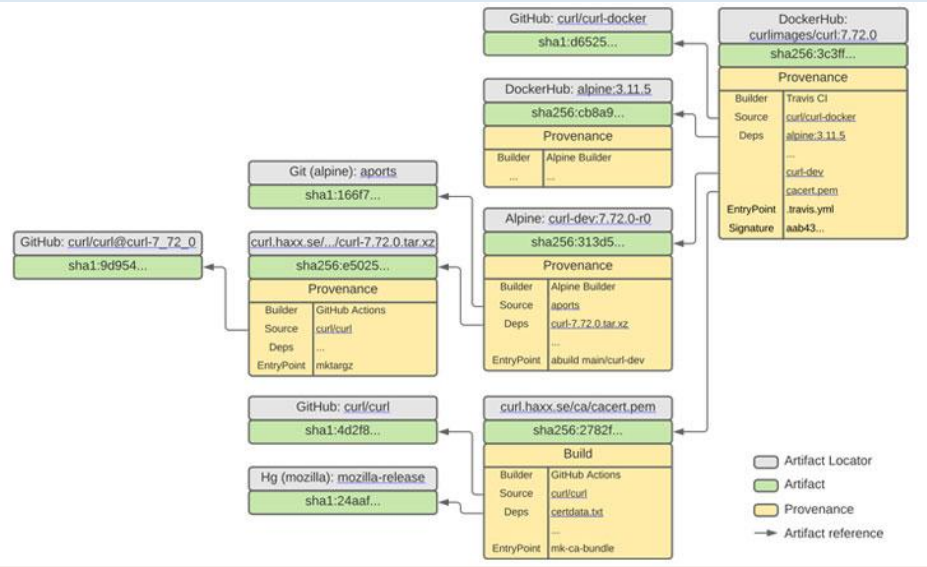
02 **源代码完整性：**确保所有代码提交都体现软件生产者的意图

- ✓ 版本控制
- ✓ 双人审核
- ✓ 永久保留源和修订记录

03 **可用性:** 确保将来可以继续构建和维护包，并且所有代码和更改历史记录都可用于调查和事件响应

- ✓ 格式
- ✓ 数字签名（真实性/完整性）
- ✓ 由构建服务生成或直接来自于构建服务，不能伪造
- ✓ 包含所有构建依赖项

遵从SLSA框架建议，确保构建和源码的完整性，确保所有证据完整且真实可信



开源社
kaiyuanshe

THANK YOU

QUESTIONS?

欢迎扫码打卡
积分可兑换对应礼品哟！

微信公众号：开源社KAIYUANSHE
视频号：开源社KAIYUANSHE
新浪微博：开源社
B站：开源社KAIYUANSHE

简书：开源社
头条：开源社
Facebook：KaiyuansheChina
Twitter：开源社KAIYUANSHE

扫码关注开源社公众号

扫码添加讲师联系方式