云原生产业大会 2021 CLOUD NATIVE INDUSTRY CONFERENCE
2021/05/26 × 中国 / 北京
原生蓄力 云领未来

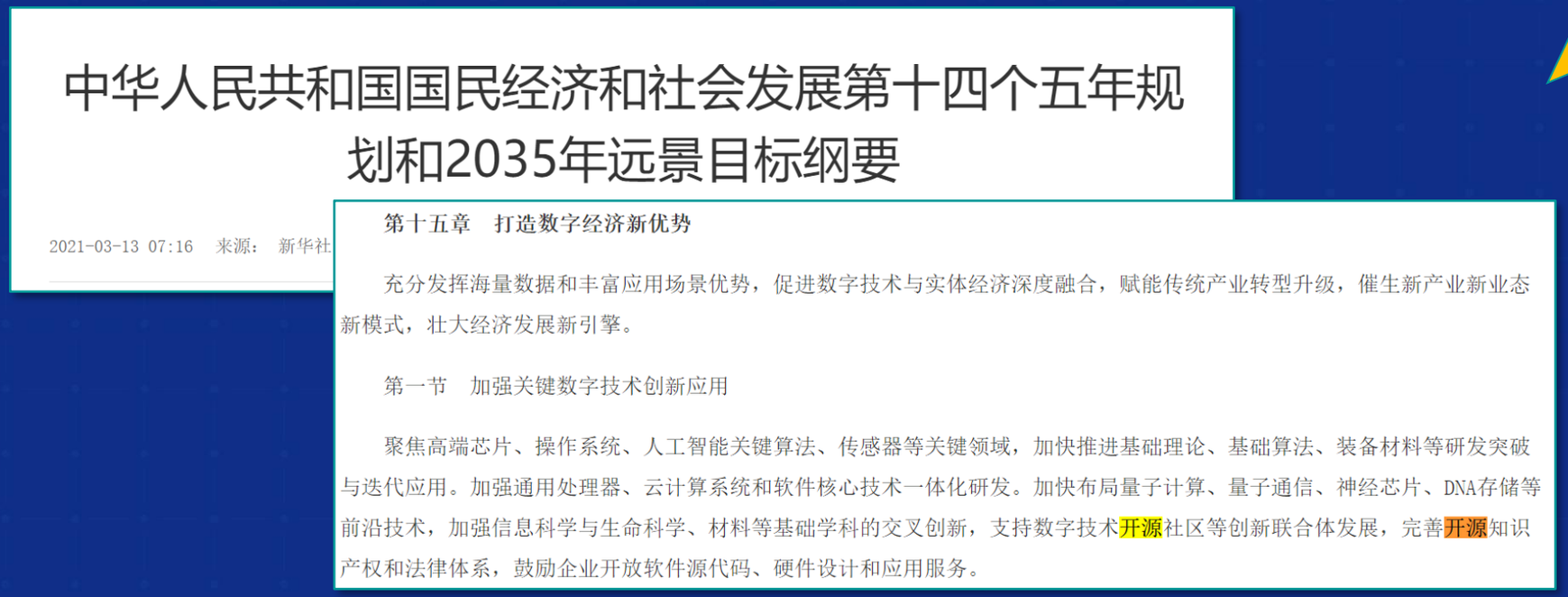
开源治理解决方案探讨

Checode 开源治理之道

CAICT 中国信通院

中国的开源发展

- 据GitHub 统计，2020年，中国开发者数量及开源贡献度增长已成为全球最快
- GitHub 预测，到2030 年中国开发者将成为全球最大的开源群体
- 众多由中国人和中国企业发起的开源项目已经逐渐成为国际主流的开源项目
- 中国本土的开源代码托管平台、开源基金会、开源组织等发展迅速
- 包括信通院在内的国家有关部门和组织正在大力支持和推动开源领域的发展



中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要

2021-03-13 07:16 来源： 新华社

第十五章 打造数字经济新优势

充分发挥海量数据和丰富应用场景优势，促进数字技术与实体经济深度融合，赋能传统产业转型升级，催生新产业新业态新模式，壮大经济发展新引擎。

第一节 加强关键数字技术创新应用

聚焦高端芯片、操作系统、人工智能关键算法、传感器等关键领域，加快推进基础理论、基础算法、装备材料等研发突破与迭代应用。加强通用处理器、云计算系统和软件核心技术一体化研发。加快布局量子计算、量子通信、神经芯片、DNA存储等前沿技术，加强信息科学与生命科学、材料等基础学科的交叉创新，支持数字技术开源社区等创新联合体发展，完善开源知识产权和法律体系，鼓励企业开放软件源代码、硬件设计和应用服务。

支持开源发展已写入十四五规划！

开源治理工作的需求来源

开源的风险和挑战

- 许可证违规&冲突
- 引入安全漏洞
- 如何满足外部的监管与审查

软件企业的内生需求

- 安全、高效使用开源软件，提高竞争力
- 避免开源软件引入的风险，保障企业自身安全

来自市场和用户的压力

- 下游客户要求软件产品中不能存在开源软件风险
- 参与开源项目、开源组织时面临的外部压力

来自外部监管的需求

- 来源于自主可控、信创等的监管要求
- 其他政策相关的监管要求

开源治理工作的主要内容

开源风险识别和管控

风险识别能力

- 基础设施（工具）的建立
- 风险识别能力与研发生命周期的结合

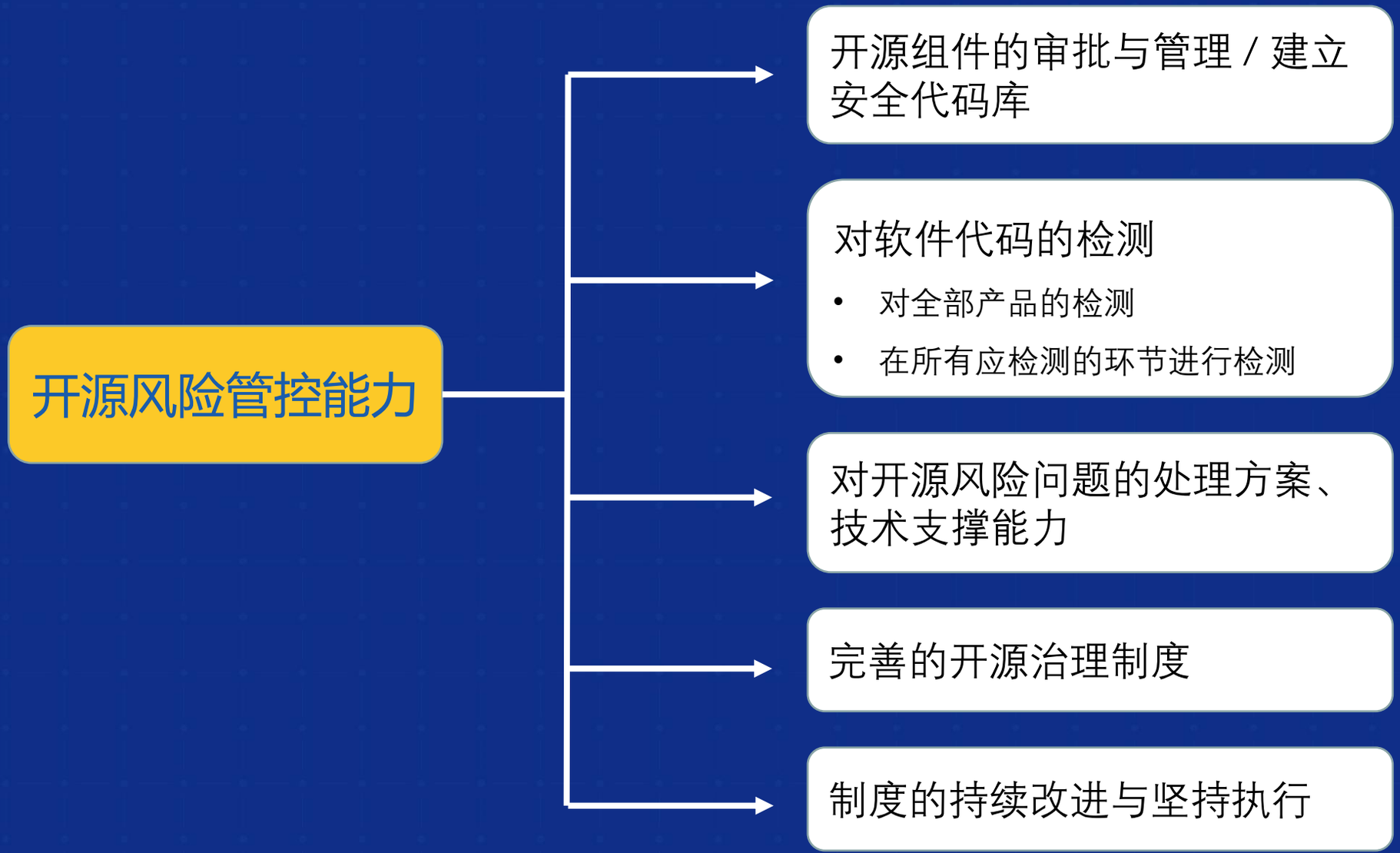
风险管控能力

- 制定风险管控策略
- 研究风险管控的方法
- 建立风险管控的制度
- 制度的调整优化与长期坚持

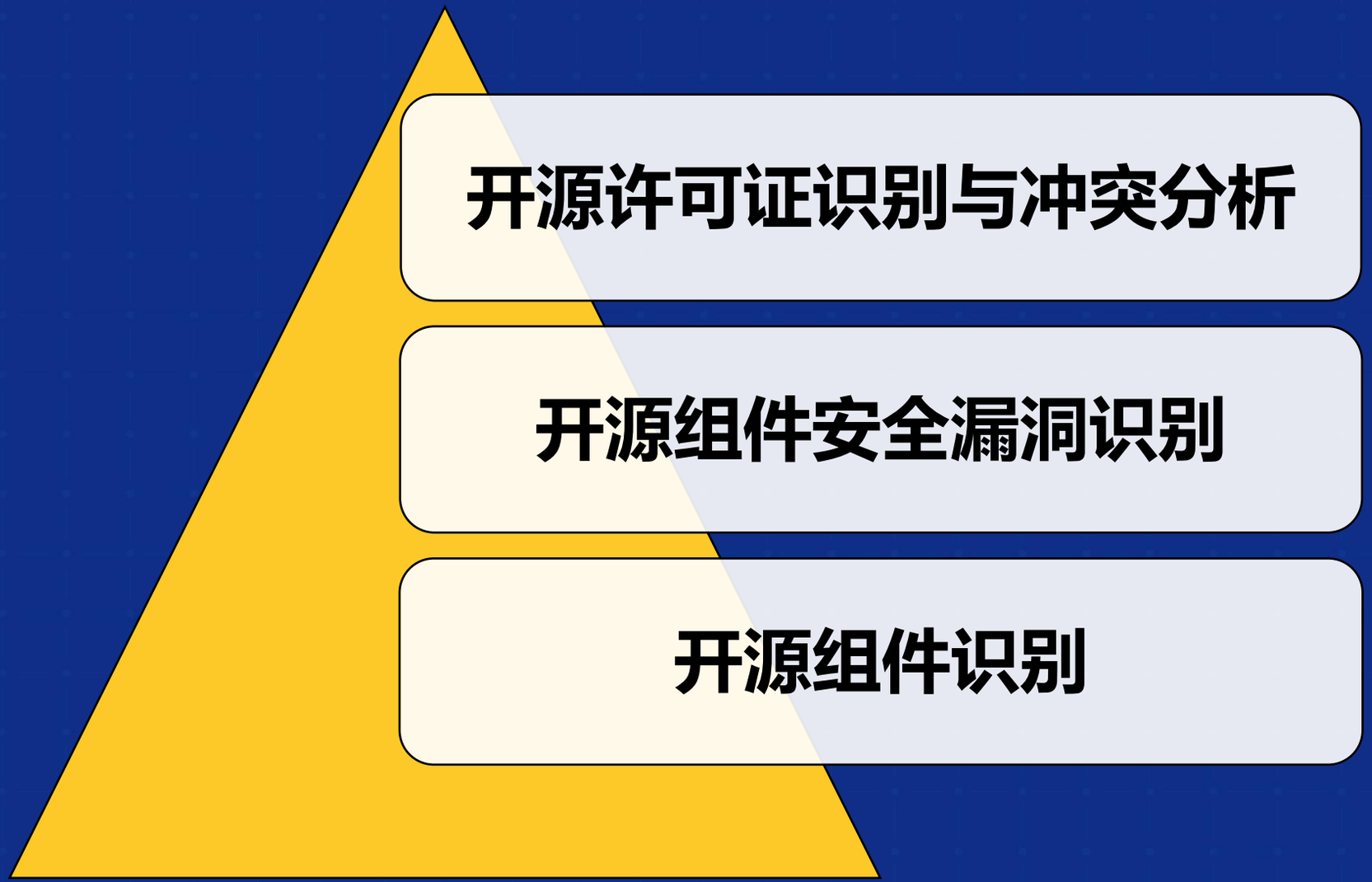
开源治理的意识

- 开源治理理念、治理制度的宣贯
- 人员培训与能力提升

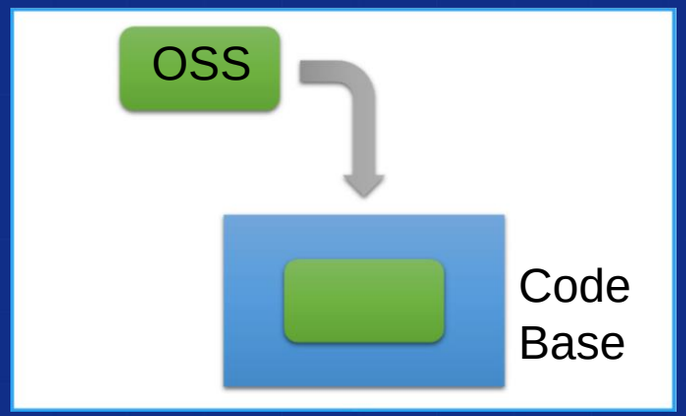
开源风险管控能力建设

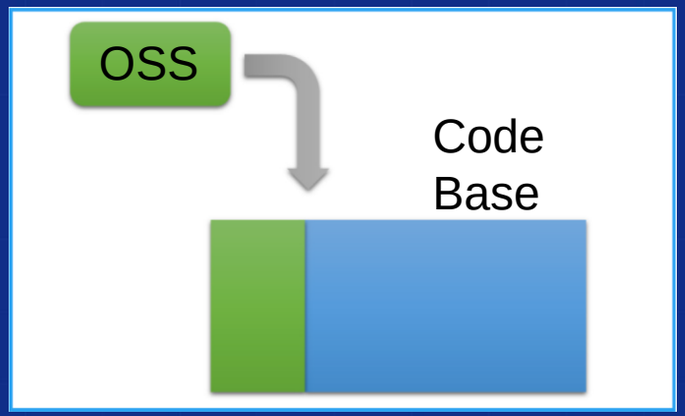

开源风险管控能力
开源组件的审批与管理 / 建立安全代码库
对软件代码的检测
对全部产品的检测
在所有应检测的环节进行检测
对开源风险问题的处理方案、技术支撑能力
完善的开源治理制度
制度的持续改进与坚持执行

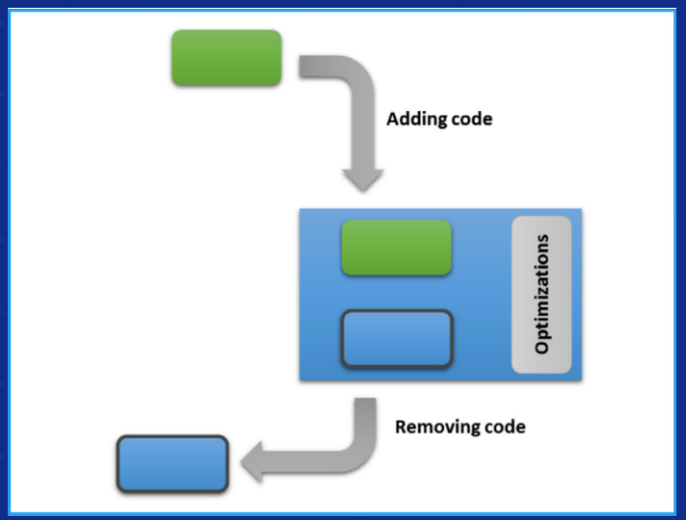
开源风险识别能力建设的目标



引用开源代码的主要方式







嵌入 / 合并（Incorporation）

- **直接**将开源组件的整体或部分**代码**加入自有软件代码当中

连接 / 依赖（Link）

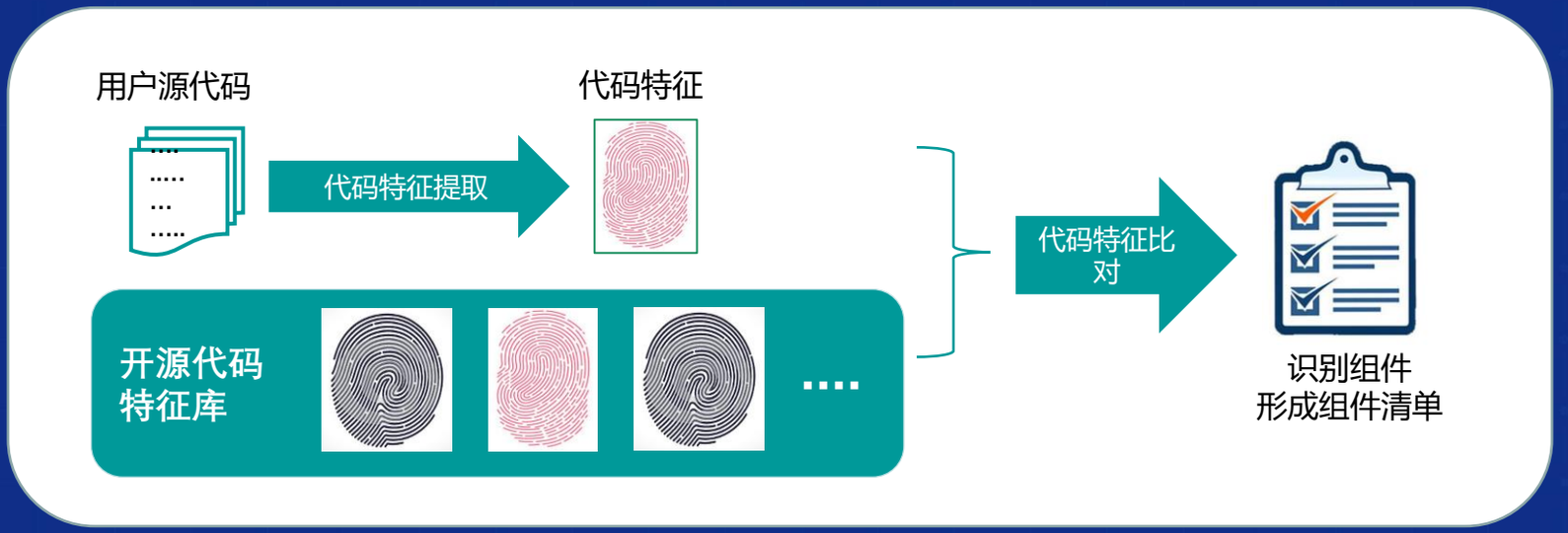
- 将**开源组件**通过**依赖、打包**等方式与自己的组件连接起来

修改（Modification）

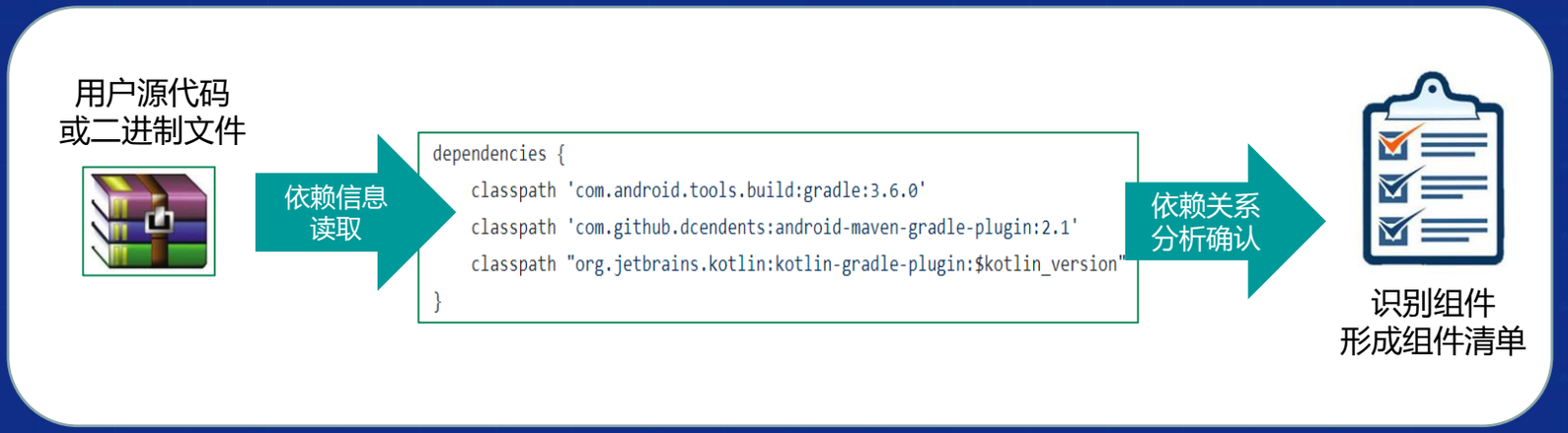
- 对开源组件的**代码**进行增加、删除、优化等**修改**之后再使用

开源组件识别技术

代码特征扫描
（代码片段扫描）



依赖关系分析



两种主流开源组件识别技术的对比

代码特征扫描（代码片段扫描）

功能特点

- 能够识别直接引用的代码，包括代码片段
- 只对被扫描代码本身进行分析，依赖的外部组件需要下载到本地进行分析
- 基本不区分编程语言
- 直接对代码本身进行分析识别，分析结果不易受到其它因素的干扰和影响

适用场景

- 测评机构进行软件测评
- 通过嵌入（Incorporation）方式直接引用开源代码的场景
- 深度使用开源，对代码有修改（Modification）的场景

依赖关系分析

功能特点

- 不分析代码本身的内容，只分析依赖关系，分析过程快速准确
- 分语言支持，对不同编程语言有不同的分析方式。
- 无法识别直接引用的代码和代码片段
- 对依赖关系信息的完整性和准确性无法进行判断，易受其它因素的干扰和影响

适用场景

- 以连接（Link）方式引用开源组件的场景
- 某些无法获取到源代码的场景
- 需要短时间内完成检测、对检测深度要求不高的场景

Checode 开源治理解决方案 —— 核心能力

- 代码特征扫描（代码片段扫描）
- 依赖关系分析
- 开源组件安全漏洞识别 & 自动通知
- 开源许可证识别 & 冲突分析
- 代码同源检测（私有库比对）
- 团队协作功能
- API 接口

Checode 开源治理解决方案 —— 关键技术

★ **源代码特征扫描**	• 领先的开源知识库 • 支持代码片段扫描识别，识别精度可调 • 扫描性能优异
★ **依赖关系扫描**	• 支持主流语言的二进制文件扫描 • 能够识别直接依赖和间接依赖
★ **安全漏洞识别**	• 先进的安全漏洞识别引擎，支持国内、国际主流漏洞库 • 及时的安全漏洞数据更新，安全漏洞更新自动通知
★ **同源代码检测**	• 先进的特征提取引擎，支持私有代码快速入库 • 进行同源扫描比对时，可以选择私有库中特定组件进行比对

Checode 开源治理解决方案的优势

★ 支持“代码特征扫描 ” 和“依赖关系扫描”两种主流开源组件识别技术

★ 支持“代码同源检测”、“开源许可证冲突分析”等特色功能

★ 领先的开源知识库

★ 支持完全离线部署和离线使用，保障用户代码安全和信息安全

★ 中文界面，符合国内用户的使用习惯

★ 提供 API 接口，方便与其它系统进行集成

★ 国产产品，自主可控，能够提供本地化技术支持服务

★ 支持客户化定制开发

云原生 产业大会

2021 CLOUD NATIVE INDUSTRY CONFERENCE

2021/05/26 × 中国 / 北京

原生蓄力 云领未来

谢谢大家!

Checode

西安奇科厚德信息科技有限公司

网址：www.checode.cn

CAICT 中国信通院