

# 中国DevOps社区峰会 2024 · 上海

10.19 | 上海龙之梦大酒店



# 源于社区 服务社区

 中国DevOps社区峰会 2024 · 上海



## 研发体系下开源安全风险发现与治理

张文凯 腾讯安全





# 张文凯

## 腾讯安全 开发安全产品负责人

- 腾讯科恩实验室开发安全产品负责人。有多年基于黑白盒代码安全测试与研究经验，目前着力于开发安全产品研发与核心能力研究，聚焦于以大数据驱动下的安全算法研究与安全产品工程化落地，专注解决来源于开源组件的软件供应链安全问题。





# 目录

- 1 来自软件供应链的安全挑战
- 2 软件供应链安全与软件成分分析
- 3 软件成分分析工具引入思路





# 01

## 来自软件供应链安全的挑战



# 软件供应链安全能力建设的趋势、必要性和监管要求

软件供应链安全指软件供应链上软件设计与开发的各个阶段中来自本身的**编码过程、工具、设备或供应链上游的代码、模块和服务的安全**，以及**软件交付渠道和使用安全**的总和。——《软件供应链安全发展洞察报告》，云计算开源产业联盟

## 泄密

隐藏“后门”，挖掘  
核心敏感数据

## 勒索

重要文件无法读取、  
关键数据损坏

## 木马

挖矿、僵尸网络、远  
程命令执行

## 劫持

在更新软件时感染病  
毒

## 有没有从根本上解决安全潜在风险？

### 行业监管与政策

《关键信息基础设施安全保护条例》  
《关于供应链安全风险提示》  
《关于规范金融业开源技术应用与发展的意见》  
《银行保险机构信息科技外包风险监督办法》  
《金融业开源软件应用 管理指南》

### 软件供应链安全趋势

- 国家级攻防演练2022-2023防守单位失陷案例60%+与软件供应链安全相关；
- 国家级攻防演练Top5攻击技战法；
- 两年持续供应链安全专项持续加大力度，是国家关注的重点；

### 建设必要性及价值

- 建立体系规范，以标准、合规、安全的组件提供给各个业务方；
- 安全左移，更早的发现和修复安全漏洞；
- 准入管理，从源头把控安全，从源头摸清楚供需、安全和管理现状；



# 软件供应链安全如何定义？



开源组件治理



软件供应链安全检查



投毒/后门检查



未知漏洞检查

.....

- 供应商提供的制品成分未知，解不开包、不知道其中有什么成分
- 开发的代码中软件成分未知，有意无意的引入未知组件
- .....



- 开源组件漏洞风险未知
- 开源组件投毒风险未知
- 开源组件许可证风险未知
- 如何发现开发中的敏感信息
- .....



- 信创替换的软件是否是安全的
- 是否能对供应商软件进行检测
- 是否做到全天候监测企业资产威胁情报信息
- .....





# 软件供应链安全：开源组件风险案例

## 开源组件漏洞风险案例：

### “太阳风暴” 攻击

2020年12月，美国企业和政府网络突遭“太阳风暴”攻击。黑客利用太阳风公司（SolarWinds）的网管软件漏洞，攻陷了多个美国联邦机构及财富 500 强企业网络。2020 年 12 月 13 日，美国政府确认国务院、五角大楼、国土安全部、商务部、财政部、国家核安全委员会等多个政府部门遭入侵。该事件波及全球多个国家和地区的 18000 多个用户，被认为是“史上最严重”的供应链攻击。



#### 关于阿帕奇Log4j2组件重大安全漏洞的网络安全风险提示

发布时间：2021-12-17 12:00 来源：网络安全和信息化部

阿帕奇（Apache）Log4j2组件是基于Java语言开发的日志记录库，被广泛用于业务系统开发。近日，阿帕奇计算系统公司发现该组件存在远程代码执行漏洞，并紧急发布安全公告提醒用户及时更新。

2021年12月16日，工业和信息化部网络安全和信息化部网络安全和信息化委员会办公室接到有关网络安全专业机构报告，阿帕奇Log4j2组件存在严重安全漏洞，工业和信息化部立即组织网络安全专业机构和网络安全专家对漏洞进行分析、研判和评估。网络安全专业机构和网络安全专家对漏洞进行了分析、研判和评估，认为该漏洞属于高危漏洞，建议用户及时更新。

### Spring 框架漏洞

2022年3月30日，国家信息安全漏洞共享平台（CNVD）收录 Spring 框架远程命令执行漏洞（CNVD-2022-23942）。攻击者利用该漏洞，可在未经授权的情况下远程执行命令，该漏洞被称为“核弹级”漏洞。使用 JDK9 及以上版本皆有可能受到影响。

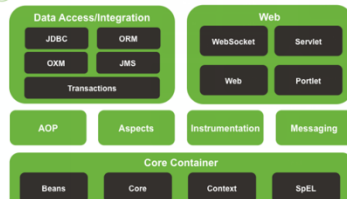


### Apache Log4j2 漏洞

2021年12月，开源组件Log4j2被发现两个相关漏洞，分别为任意代码执行漏洞和拒绝服务攻击漏洞，攻击者可以通过构造特殊的请求进行任意代码执行，以达到控制服务器、影响服务器执行的目的。该漏洞已影响超6万个开源软件，涉及相关版本软件包32万余个，被认为是“2021年最重要的安全威胁之一”



#### Spring Framework Runtime



### XZ 后门事件

2024年3月29日，软件开发Andres Freund报告称，liblzma库在2024年2月发布的5.6.0和5.6.1版本中，包含的Linux实用程序xz含有一个恶意引入的后门。虽然大多数Linux发行版都安装了xz，但后门仅针对基于Debian和RPM的x86-64架构系统。在发现时，后门版本尚未被广泛部署。

## 开源组件许可证风险案例：

- 2021年4月30日，罗盒公司状告风灵公司侵权获赔50万元，同时要求风灵公司停止侵权行为。在该案件中原告罗盒公司，独立开发“罗盒(Virtual App)插件化框架虚拟引擎系统 V1.0”（简称VirtualApp V1.0），在2016年引入GPL 3.0 许可证，于2017年取得计算机软件著作权登记证书，且声明用于商业用途请购买商业授权。2018年原告发现名为“点点桌面”的软件使用了 VirtualApp V1.0 的代码，经过源码分析对比，发现两者之间高度相似，遂起诉被告福建风灵公司。经法院审判被告赔偿原告为制止侵权行为而支出的合理费用50万元。此次判决是中国首个明确 GPL 3.0 许可证具有法律效力的案例。
- 2021年12月，抖音海外版 TikTok 上线了一款名为 TikTok Live Studio 的 APP，但不久其下载页面就被删除。TikTok 官方对此事做出回应，原因是该 APP 违反 GPL 许可证，其使用 GPL 许可证下的开源软件源码，却没有按照 GPL 许可证要求开源。

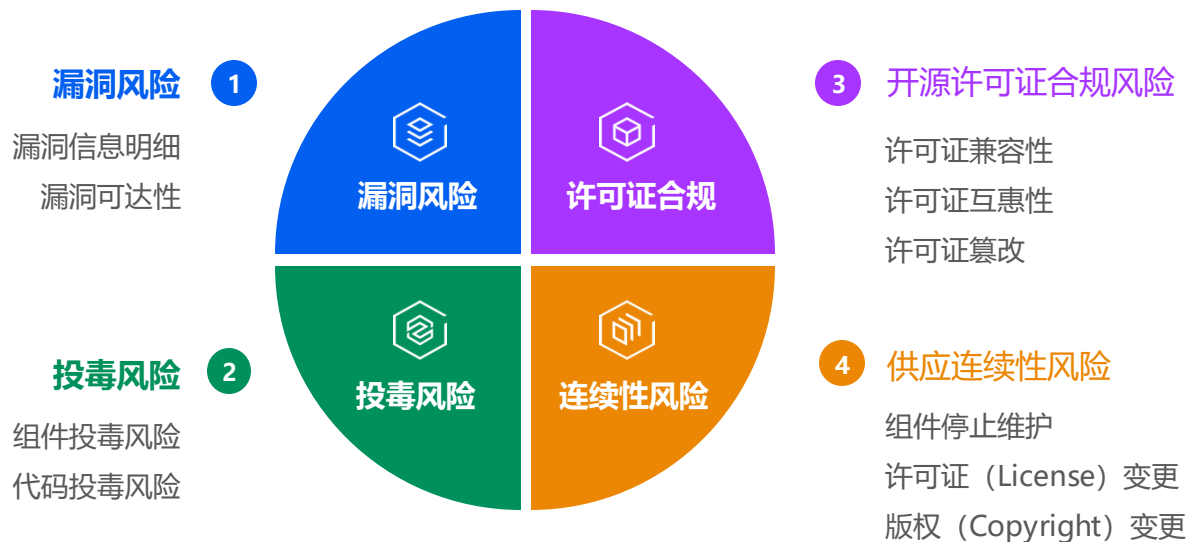






# 《软件成分分析系统安全技术要求与测试评价方法》

## 开源组件挑战



## 自主可控要求

核心数据可控

核心能力自研

国产化环境支持



# 企业在开源组件治理上存在的痛点

## 01 缺乏SCA能力体系建设

- 源码SCA能力建设
- 制品SCA能力建设
- DevOps上缺乏安全左移能力
- DevOps安全能力建设尚在规划

## 02 缺乏开源风险预警能力

- 核弹级开源组件漏洞风险预警
- 日常扫描中的开源风险发现
- 缺乏对风险处置给出专业意见
- 缺乏实时的开源组件知识库

## 03 缺乏制品准入能力建设

- 缺乏对第三方制品风险发现能力
- 缺乏制品入库前的风险监测
- 信创替换软件是否真的安全
- 组件黑白名单/质量红线建立

## 01 难在SCA能力未全覆盖

- 源码SCA能力接入
- 制品SCA能力接入
- 分析能力受限，漏报多
- 无法满足对特定扫描项的需求

## 02 难在组件/漏洞修复复杂

- 组件升级不知哪个版本更好
- 漏洞修复缺少详细的推荐方案
- 漏洞修复的优先级怎么制定
- 缺少业内成熟实践过的修复经验

## 03 难在SBOM台账风险运营

- 如何建立企业级的SBOM
- 如何基于SBOM进行台账运营
- 新发现风险如何快速定位
- SBOM数据的长期运营和维护

企业在开源组件治理上存在能力建设缺乏、检测覆盖度不足、风险修复困难以及SBOM难运营等痛点。





# 02

## 软件供应链安全与软件成分分析



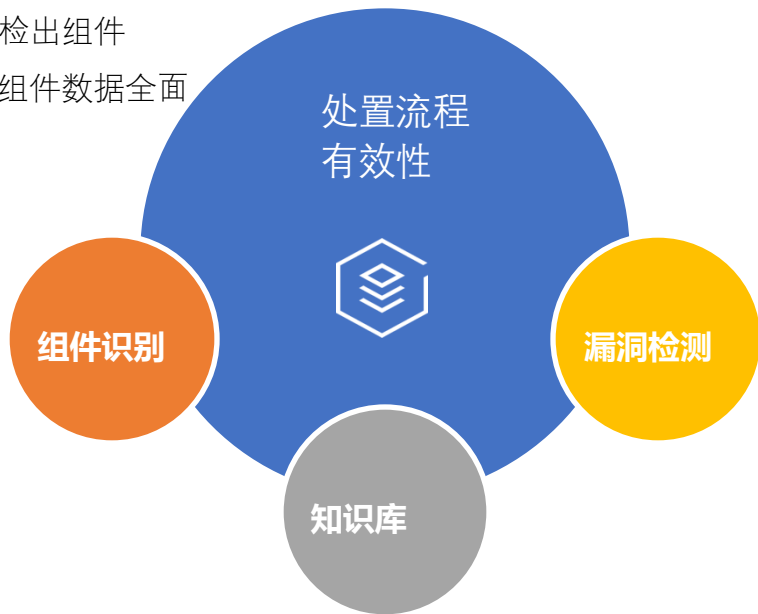
# 研发角度看软件供应链安全问题

- 开源组件问题突出：SCA工具的引入是首要优先级



# 软件成分分析核心挑战

- 底层分析能力：完备且详细的检出组件
- 多维度数据：组件定位精准、组件数据全面



## 组件检出能力覆盖

组件检出准确度保证

组件版本检出准确度保证

组件识别能力组合：

- 制品扫描 – 包管理器识别
- 制品扫描 – 二进制SCA
- 静态包管理器识别
- 动态包管理器识别
- 代码片段级识别

开源组件知识库数据处理

漏洞知识库修正（NVD等数据源数据错误）

多数据源数据汇聚（NVD、CNVD、GHSA等）

开源组件许可证监控（真实代码仓库监控）

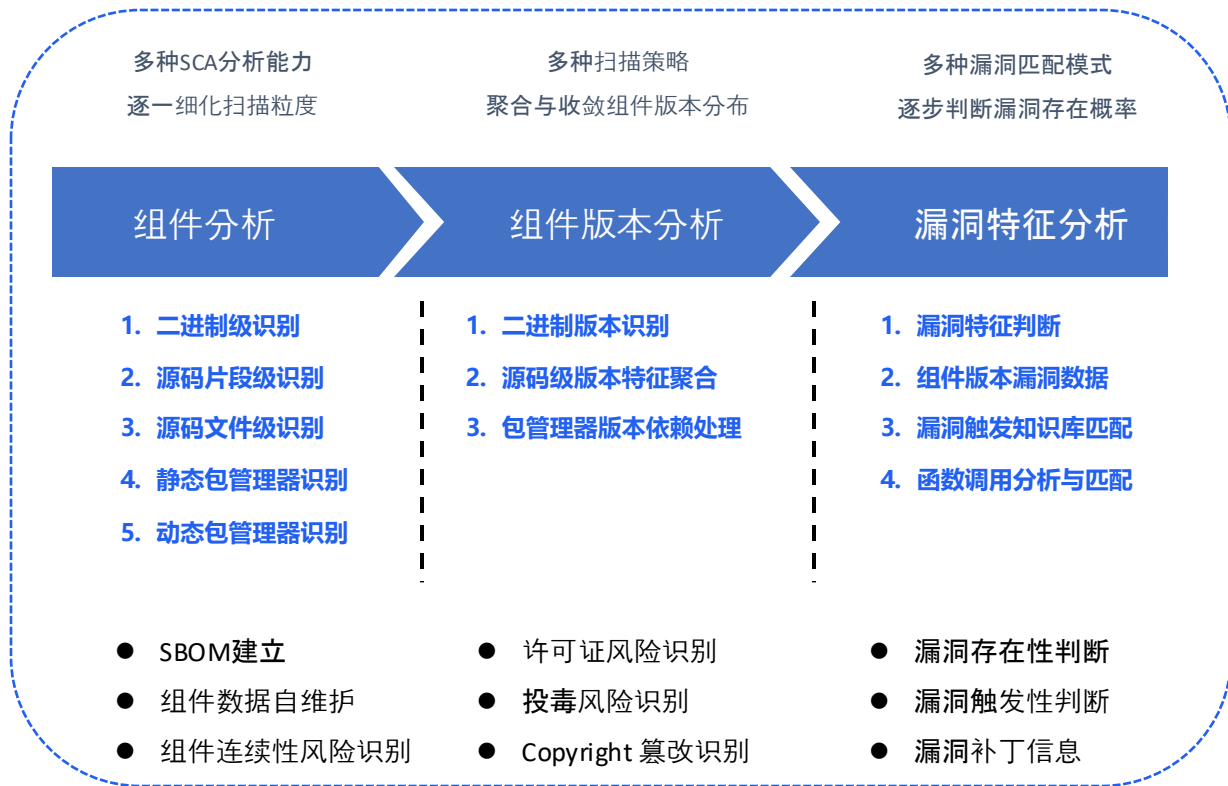
代码克隆类型	置信等级
TYPE-1	句法克隆，去除空格，空行和注释后，完全相同
TYPE-2	句法克隆，除了对一些unique identifiers（函数名，类名，变量）重命名以外，完全相同
TYPE-3	句法克隆，片段部分被修改，如添加或删除了部分代码片段，或是重新排序了部分代码片段
TYPE-4	句法克隆，语义相似，但句法不相似（非常难检测）

## 漏洞可达性

分类	状态	置信等级
触发性	可触发 不可触发	A - 人工确认
		B - SCA工具可触发验证（代码级）
存在性	存在 疑似存在 不存在 已修复	A - SCA工具存在性验证（代码级）
		B - SCA工具存在性验证（组件级）



# 软件成分分析多阶段示意



多SCA阶段组合  
深入解决供应链  
风险

各阶段逐步深入  
分析  
提升结果置信度

下游任务识别





# 03

## 软件成分分析工具引入思路





# 开源治理接入总览

代码托管

代码编写

单元测试

构建部署

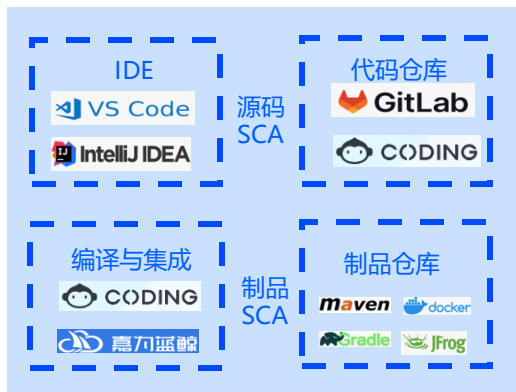
集成测试

制品管理

持续部署

常态化运营

研发整合/开发接入



制品归档/软件准入



安全管理/台账运营



推修优化/组件治理



⚡ 开源组件检查

🔍 漏洞风险发现

📁 BOM资产梳理

🔄 运行态SCA检测

🌌 供应连续性检查

⚠️ 组件风险情报

📄 间接依赖分析

📄 敏感信息审查

🛡️ License合规审计

💻 病毒文件检测

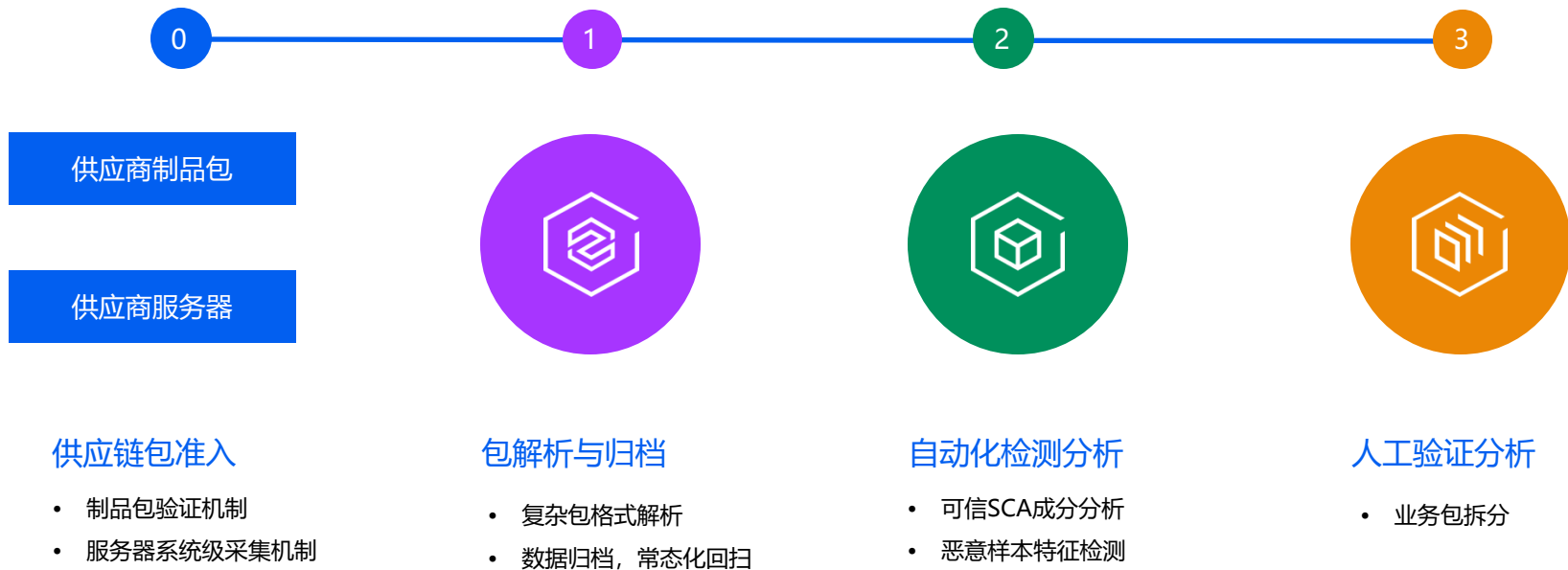
📋 系统高稳定性

🔍 知识库快速查询



# 软件成分分析工具在软件供应链准入场景下应用

- 基于实战经验的分析平台：包归档、元信息提取
- 充分发挥二进制SCA：解包能力强、二进制分析对象兼容性高
- 系统采集能力：完整采集运行时数据，综合SCA分析



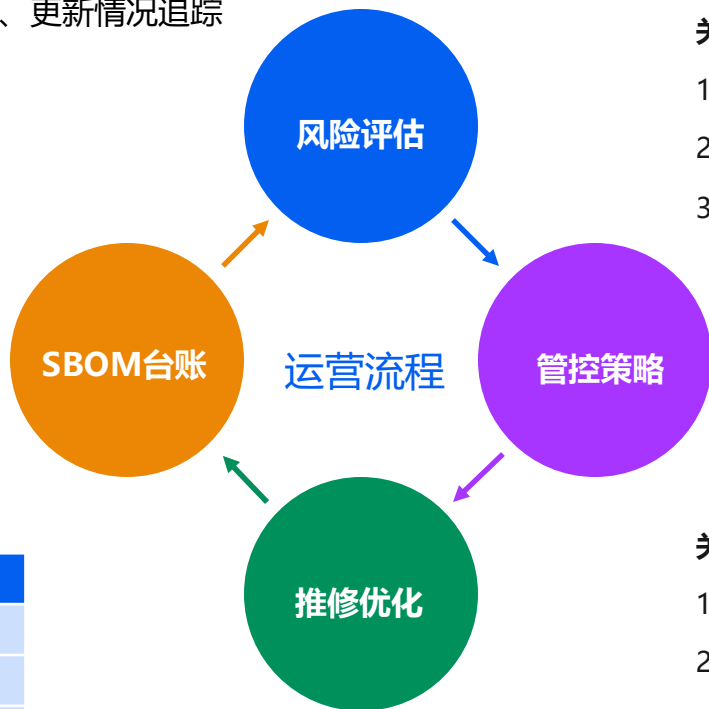
# 软件成分分析工具在开源组件治理场景下的流程

- SBOM台账建立：自动化生成、信息全面
- SBOM台账运营：组件搜索、更新情况追踪

## 关键技术点

1. 组件定位能力
2. 组件检测、附加信息能力
3. 组件管理能力

定位字段	说明
定位	PURL相关字段
作用域	dev、test、compile区分
检出依据	工具检出依据



## 关键技术点

1. 安全风险：漏洞
2. 合规风险：许可证风险
3. 综合风险：组件版本分布、连续性问题

## 关键运营策略

1. 漏误报运营能力：结果屏蔽、修正
2. 管控策略能力：黑白名单机制
3. 灵活API能力



# 源于社区 服务社区

## THANKS!

