网络安全 FCIS 2023 创新大会

从源头预防：移动终端软件供应链安全治理探讨

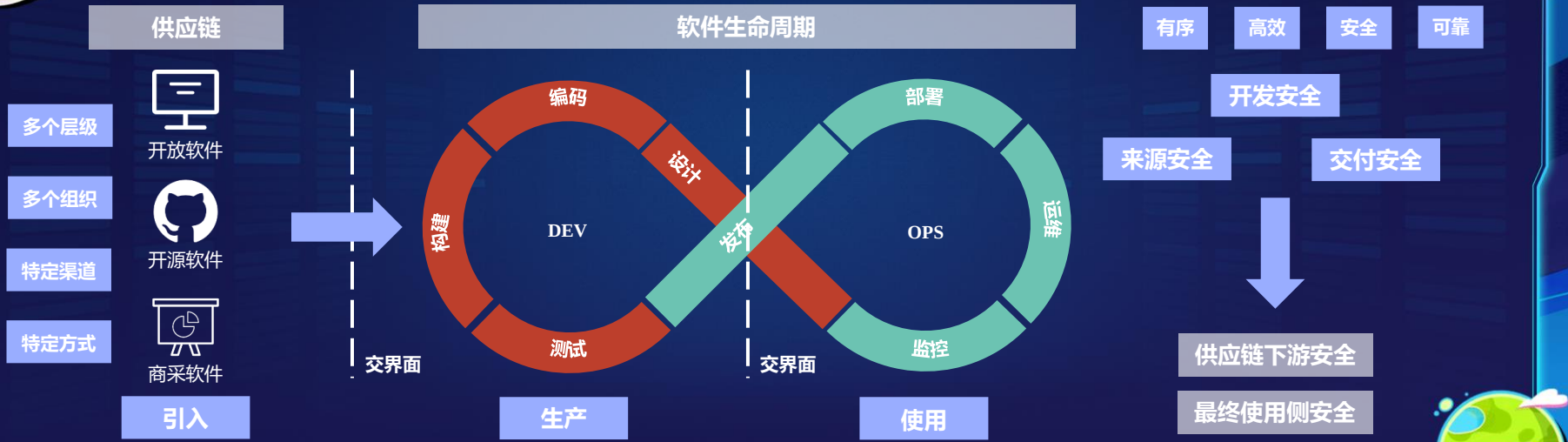
vivo安全研发工程师 刘津铭

FREEBUF

目录

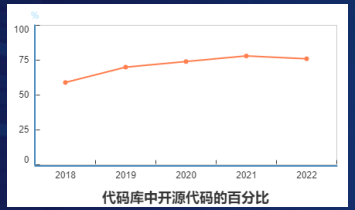
01 软件供应链安全发展趋势

软件供应链及软件供应链安全的定义



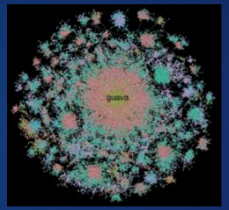
软件供应链发展趋势及面临安全风险

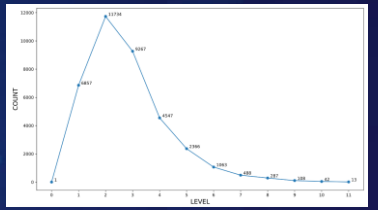
趋势①：开源软件逐步成为软件供应链基础设施



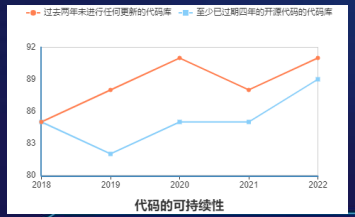
代码库中开源代码的百分比

趋势②：随着供应链链条增长，软件复杂度增加



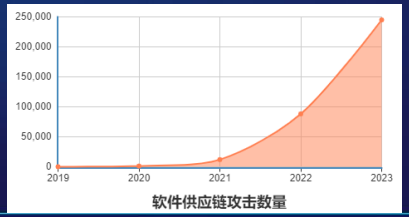


风险①：开源代码的可持续性下降，开源代码的质量难以把控

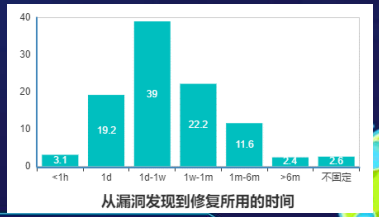


代码的可持续性

风险②：软件供应链链条越长攻击面越大，完整性遭受挑战



软件供应链攻击数量



从漏洞发现到修复所用的时间

数据来源：新思科技《2023开源安全和风险分析报告》

02 移动端软件供应链治理痛点

移动端软件供应链安全治理痛难点

例：CVE-2023-4863缓冲区溢出影响广泛排查难度高

- Libwebp 是谷歌提供用于编码和解码 WebP 格式图像的库

- 排查对象是构建后的应用、制品，且通过多重依赖引用Libwebp制品，缺少源码，二进制排查难度高

软件供应链来源广泛

管理难

多重依赖关系复杂

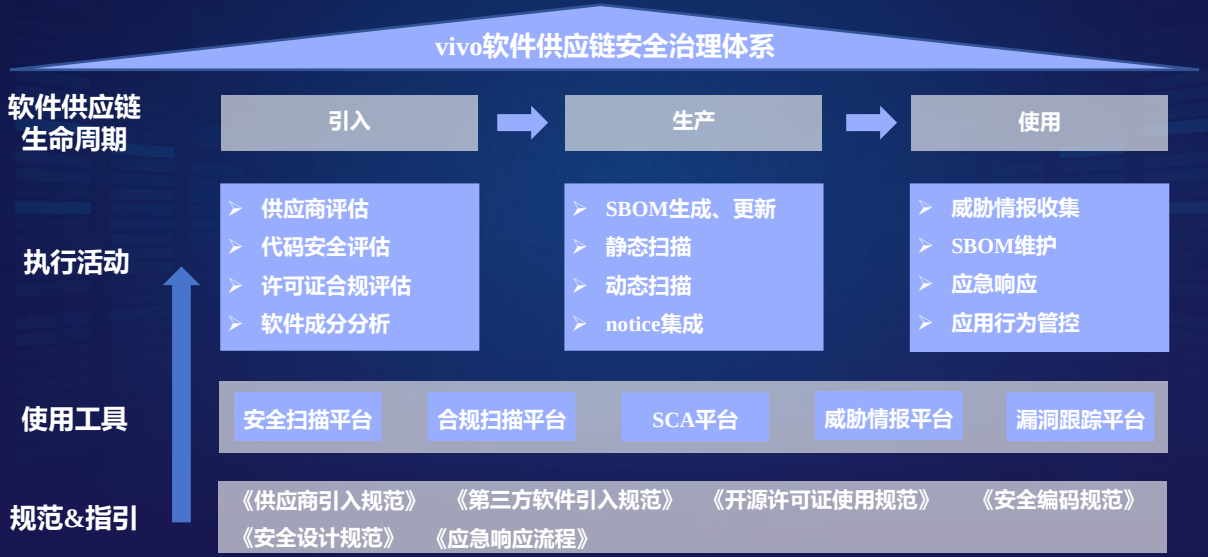
排查难

制品对用户完全可见

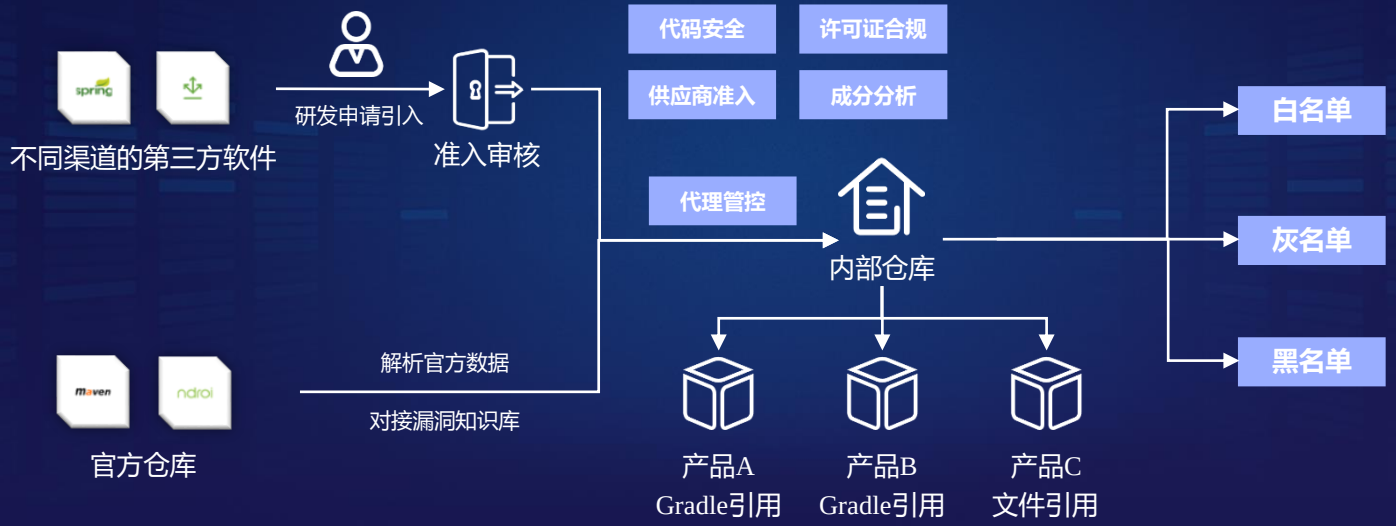
不可控

03 vivo软件供应链安全治理实践

vivo软件供应链安全治理实践



引入环节：建设组件管理平台统一管控



生产环节：多模态行为主体识别精准分析

组件管理平台对制品管控能力强，对源码方式引入的第三方软件管控能力弱

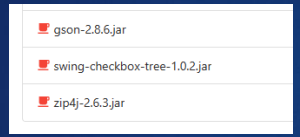
多模态行为主体识别：精确识别代码文件归属，提升软件成分分析准确性，为软件供应链安全治理提供数据支撑

生产环节：多模态行为主体识别精准分析

源代码检测技术：通过包管理器、代码片段、精确文件/目录识别

```
14  import java.io.IOException;
15
16  import okhttp3.Call;
17  import okhttp3.OkHttpClient;
18  import okhttp3.Request;
19  import okhttp3.Response;
```

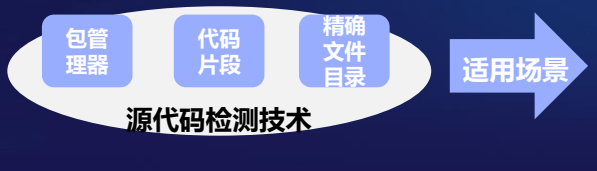
代码片段识别



精确文件识别

```
31  dependencies {
32
33      implementation 'androidx.appcompat:appcompat:1.6.1'
34      implementation 'com.google.android.material:material:1.9.0'
35      testImplementation 'junit:junit:4.13.2'
36      androidTestImplementation 'androidx.test.ext:junit:1.1.5'
37      androidTestImplementation 'androidx.test.espresso:espresso-core:3.5.1'
38  }
```

包管理器识别



生产环节：多模态行为主体识别精准分析

制品检测技术：通过代码路径特征、函数特征、文件特征、哈希特征、manifest特征等多维度识别

生产环节：多模态行为主体识别精准分析

制品检测技术：通过代码路径特征、函数特征、文件特征、哈希特征、manifest特征等多维度识别

多模态行为主体识别已覆盖vivo软件开发全流程，日均提供识别能力6000+次

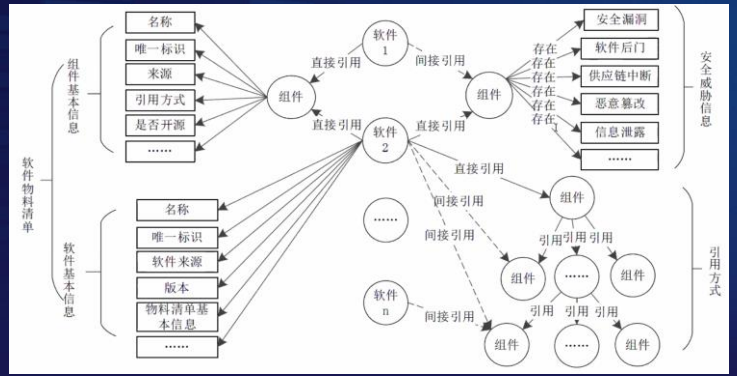
对APK制品检测进行横向测试，vivo基于**自研多模态行为主体识别能力，检出效果好**

	vivo	检测平台A	检测平台B
应用A	162	149	130
应用B	68	60	45
应用C	145	132	118

同应用第三方软件检出数量

使用环节：SBOM助力软件供应链风险治理

软件物料清单（SBOM）：描述软件包依赖树的一系列元数据集合，包括组件唯一标识、供应商、版本号、组件名、版权、许可证、安全威胁等多项关键信息，旨在跨组织共享，提升软件透明度



- 201812：美国《联邦采购供应链安全法案》
- 202102：美国《美国供应链行政令》
- 202105：美国《关于改善国家网络安全的总统行政命令
- 202107：欧盟《供应链攻击威胁情景》报告
- 202209：欧盟《网络弹性法案》
- 《软件供应链安全能力成熟度参考模型》（草案）
- 《软件供应链安全要求》（草案）

资料来源：《信息安全技术 软件供应链安全要求》

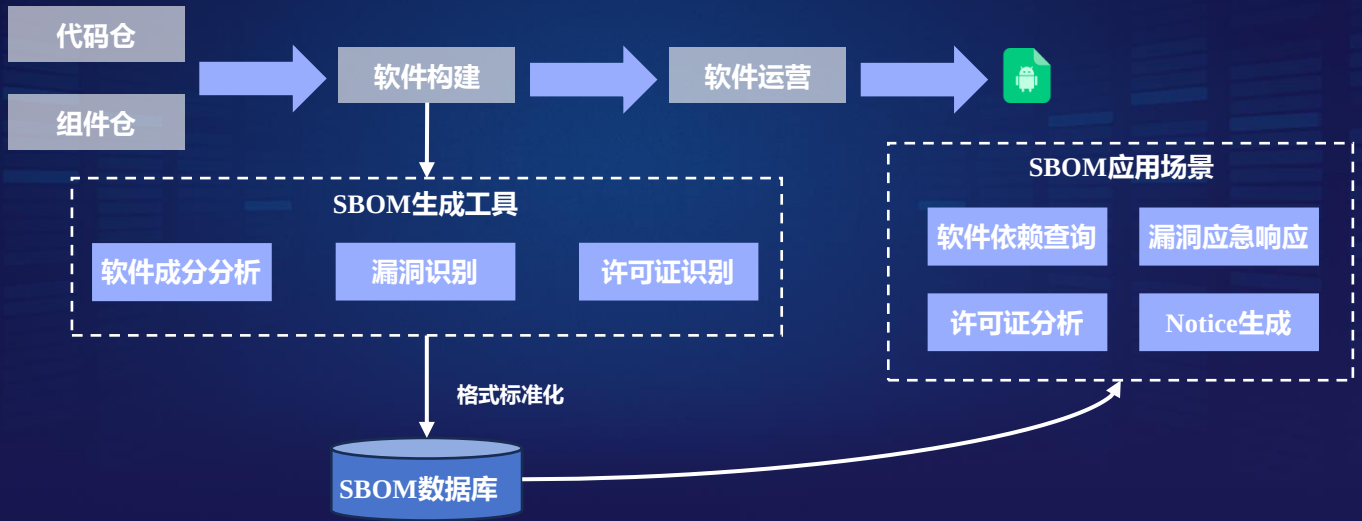
使用环节：SBOM威胁情报能力推进应急响应

威胁情报是软件供应链安全治理的基础，是应急响应流程的核心

开源组件漏洞数据不足以覆盖软件供应链安全风险治理工作，多渠道整合威胁情报管控软件供应链安全

- 覆盖maven、gradle、npm、pypi等**技术栈**
- 覆盖**35w+条风险数据**，内部情报1000+条
- 威胁情报更新时间控制在**小时级**
- 构建资产搜索引擎，**毫秒级**检索影响资产

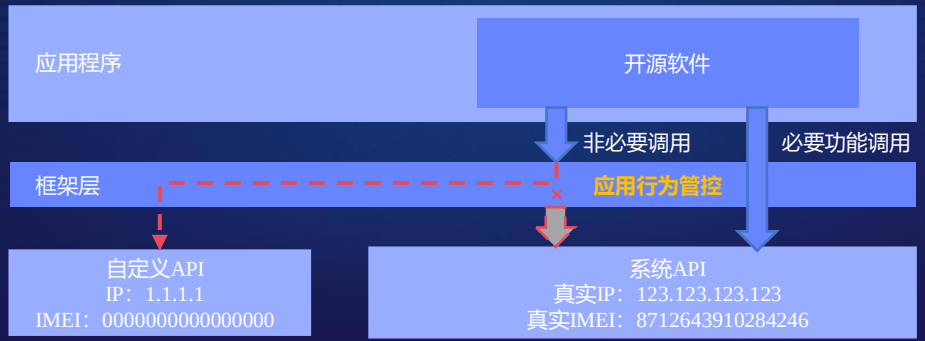
使用环节：SBOM助力软件供应链风险治理



使用环节：应用行为管理

应用行为管理：判断应用程序意图，最小化应用程序权限，最大化守护安全隐私底线，保障软件供应链安全

例：某开源软件存在获取设备信息等行为，经深度评估为不满足权限最小化原则，但由于不得不使用该第三方软件，且对开源代码修改存在许可证合规的风险，从系统底层切断该开源软件采集用户终端数据的通道



04 探讨与未来展望

探讨与未来展望

- 分享vivo软件供应链安全治理经验，携手共建多模态行为主体识别能力，从源头堵住供应链安全隐患
- 参与软件供应链治理社区建设，推动建立完善的漏洞相应机制，提升供应链安全风险应急响应能力

网络安全 FCIS 2023 创新大会

THANKS

FREEBUF

关于vivo千镜

秉承“数据安全与隐私保护是用户的基本权利，vivo必须全力保障”的底线原则，首创千镜可信引擎 +，赋能各行业合作伙伴，守护各大业务场景，为亿万用户的数字化生活保驾护航

扫码了解更多vivo安全资讯