2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

企业级 DevSecOps
开源治理方案演进之路

快速发布 谁与争锋

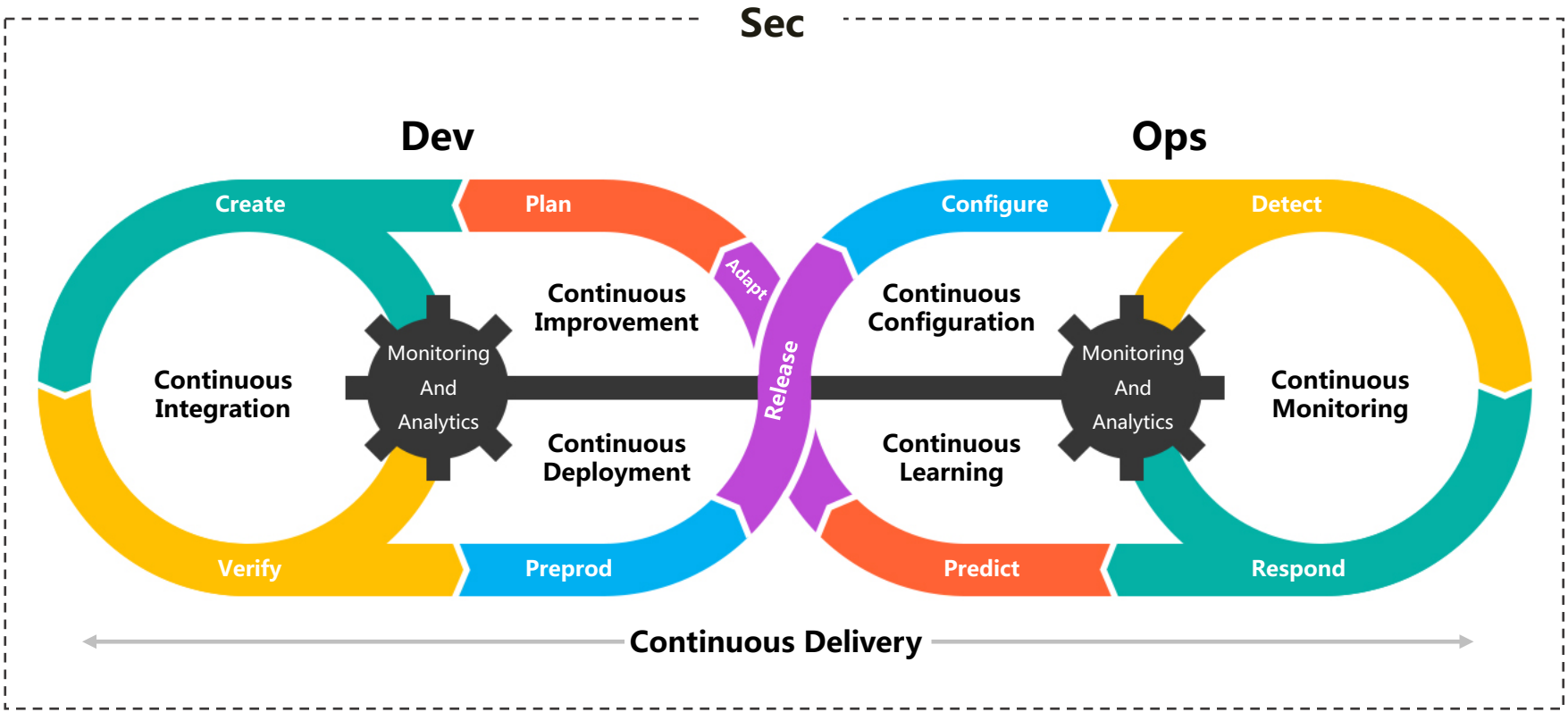
THE SPEAKER

刘永强

JFrog 中国解决方案架构师

- 云计算平台
- 生命周期管理
- 容器化
- 持续交付-DevOps
- 社区实践
- Arch Summit，DevOps Summit
- DevOpsDays，Qcon大会嘉宾

DevSecOps 闭环



开源不等于安全

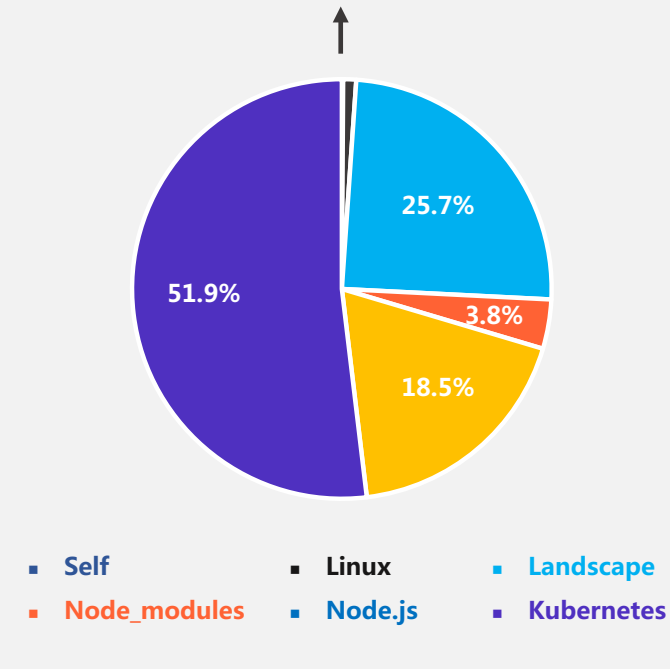
开源 != 安全

- 开源组件几乎没有安全测试
- 提供方没有安全意识
- 安全问题需要投入更多的研发成本
- 组件使用者不关心第三方组件代码
- 一个漏洞，影响范围广
- 开源社区分享精神，维护者轻易把项目管理权交给其它人员
- 黑客的目标一般是开源组件
- 78% 的漏洞存在于间接依赖关系中
- 2000年～2020年社区发展

商业 != 安全

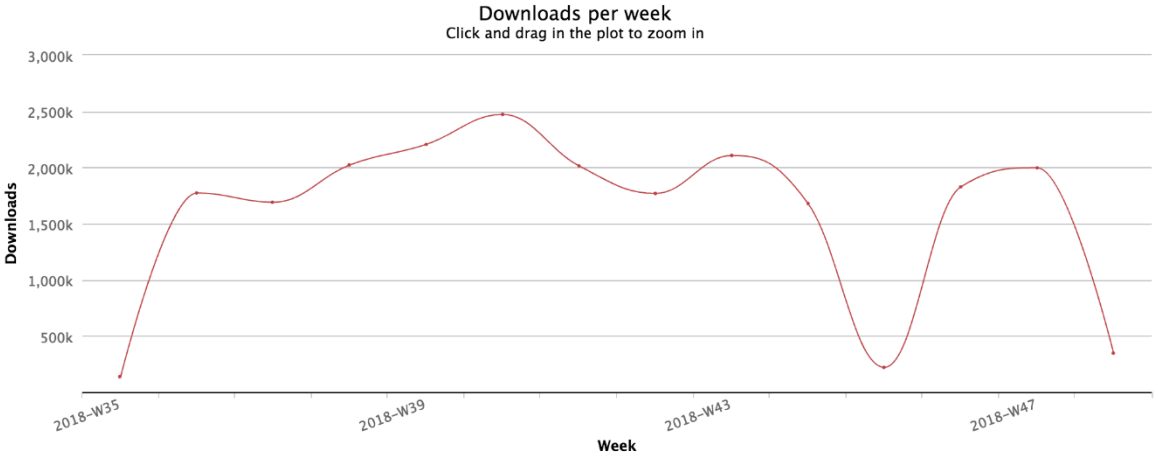
- 商业软件依赖开源(被动依赖)
- Linux: redhat, Suse
- Openstack
- Kubenates
- Hadoop

我们的代码 <0.1% 在整个软件中



Npm：event-stream事件

event-stream包是一个Node.js流数据的JavaScript软件包。起因是 event-stream 项目的作者由于时间和精力有限，将其维护工作交给另一位开发者 Right9ctrl，该开发者获得了event-stream的控制权，将恶意代码注入。注入的恶意代码将会窃取比特币用户钱包内的私钥并发送至一个域名。

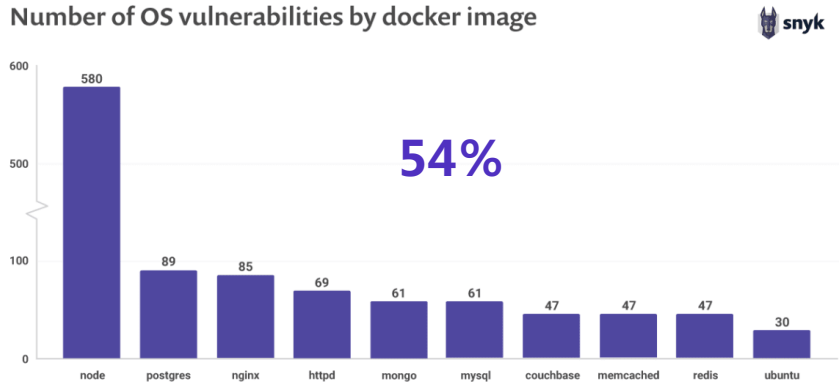


- 周下载量在**200万+次**
- 持续时间为**2.5个月**
- 大约**2000万+**次的下载量
- 其他**开源组件**也有依赖

各种语言的漏洞情况

Heartbleed

Shellshock



30% Docker 镜像
包含已知漏洞

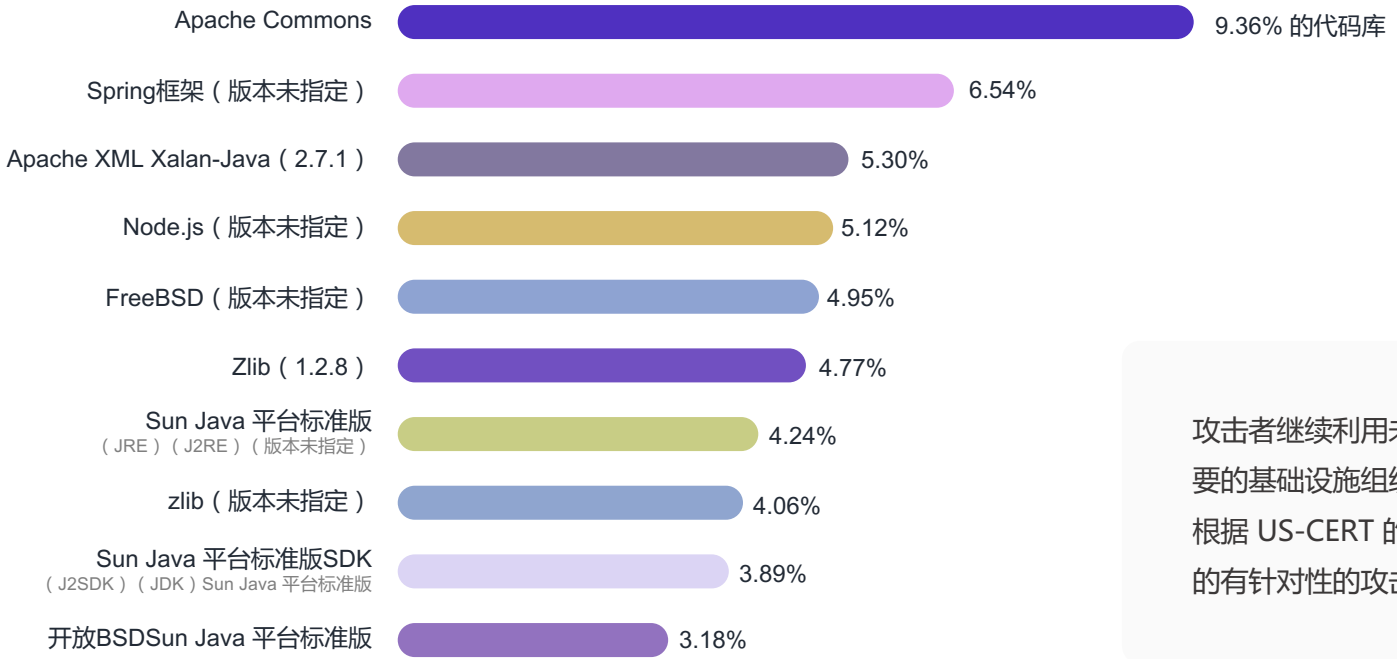
14% Npm package
包含已知漏洞

59% Maven 已发现
漏洞仍未修复

开源软件安全漏洞风险

2019 开源安全报告（Snyk）：开发者安全技能短板明显，热门项目成漏洞重灾区！

已发现十大高风险组件



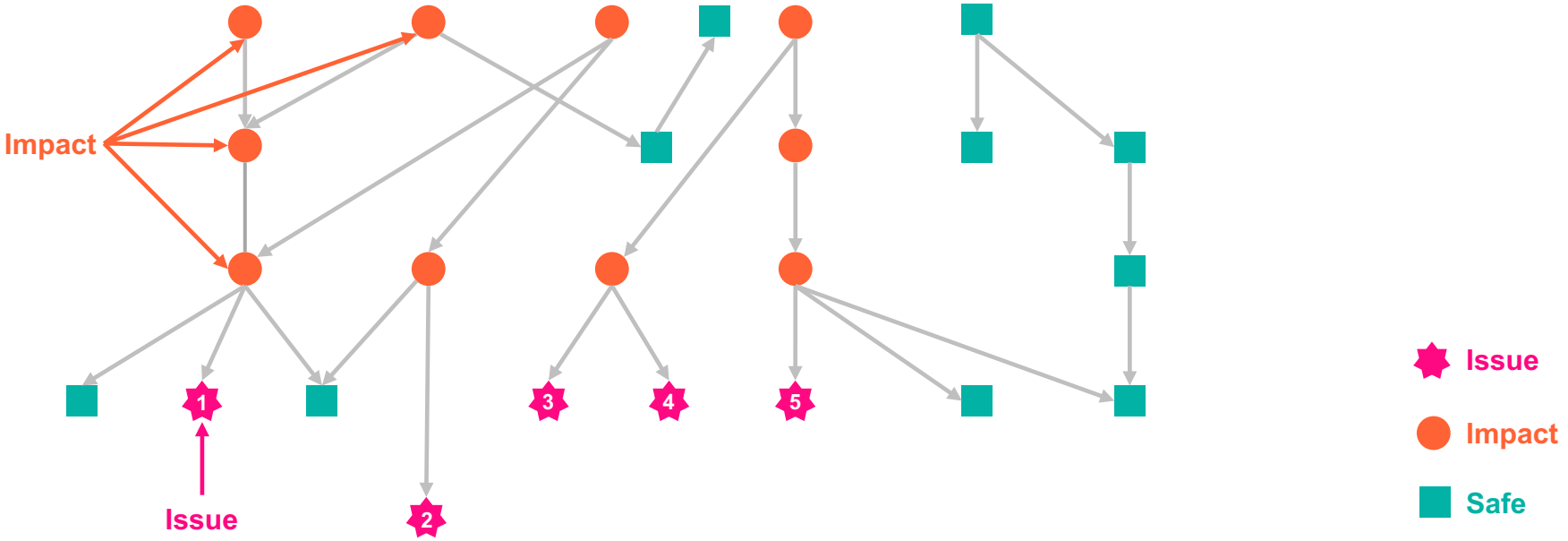
攻击者继续利用未打补丁的软件对重要的基础设施组织进行攻击。
根据 US-CERT 的统计，多达 85% 的有针对性的攻击是可以预防的。

Register to Security Alerts

Platform Specific	Broad Lists
Ubuntu	US-CERT
Node.js	NVD
OpenSSL	OSVDB
(your vendor sec list)	

第三方组件安全管控难点

无法定位问题影响范围 -- 精准分析难



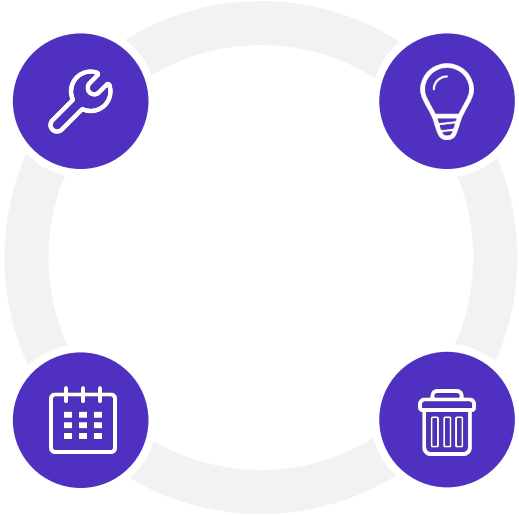
企业开源治理痛点

大多数企业缺少开源组件及软件的协议分析、漏洞评估及修复能力

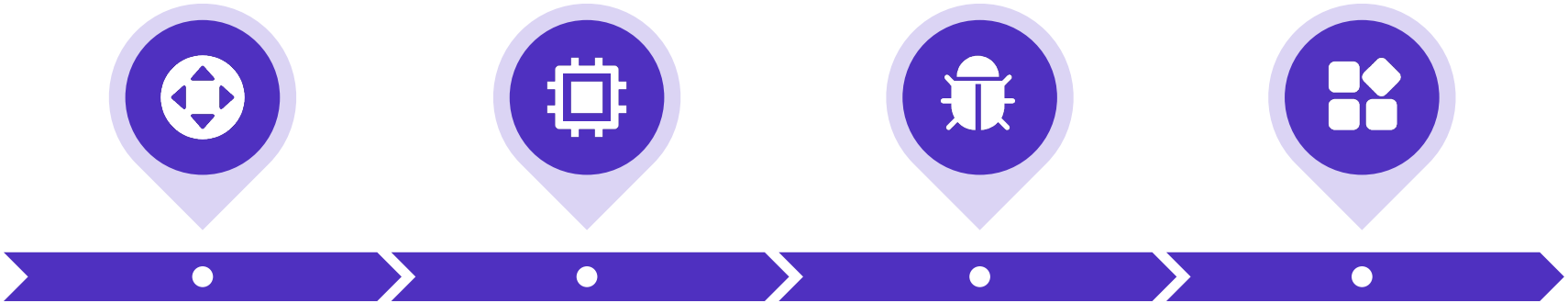
企业使用开源软件缺乏安全评估、法务评估和引入流程

企业不清楚项目中使用了多少开元软件和开源组件

企业在开元软件或组件出现漏洞时，无法快速定位到漏洞组件的影响范围，并及时止损，禁止漏洞组件下载



如何管控治理？



统一入口 & 控制源头

jcenter，dockerHub 等大的第三方源站

依赖组件分析管理

通过搭建内网私服制品哭统一管理并通过构建工具进行组件分析

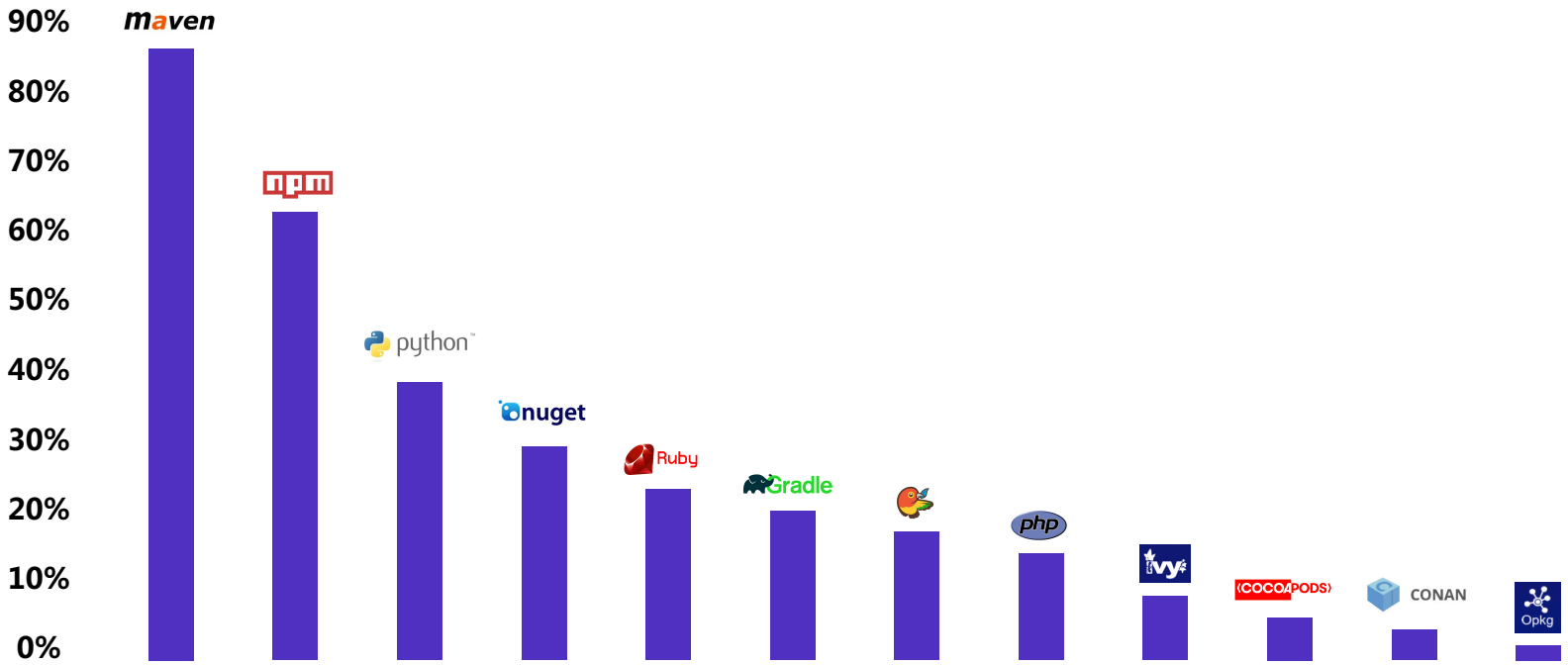
漏洞数据源

NVD、CNVD、VlunDB

安全左移 & 全生命周期管理

从开发、构建、部署、运行进行全生命周期管控 & 治理

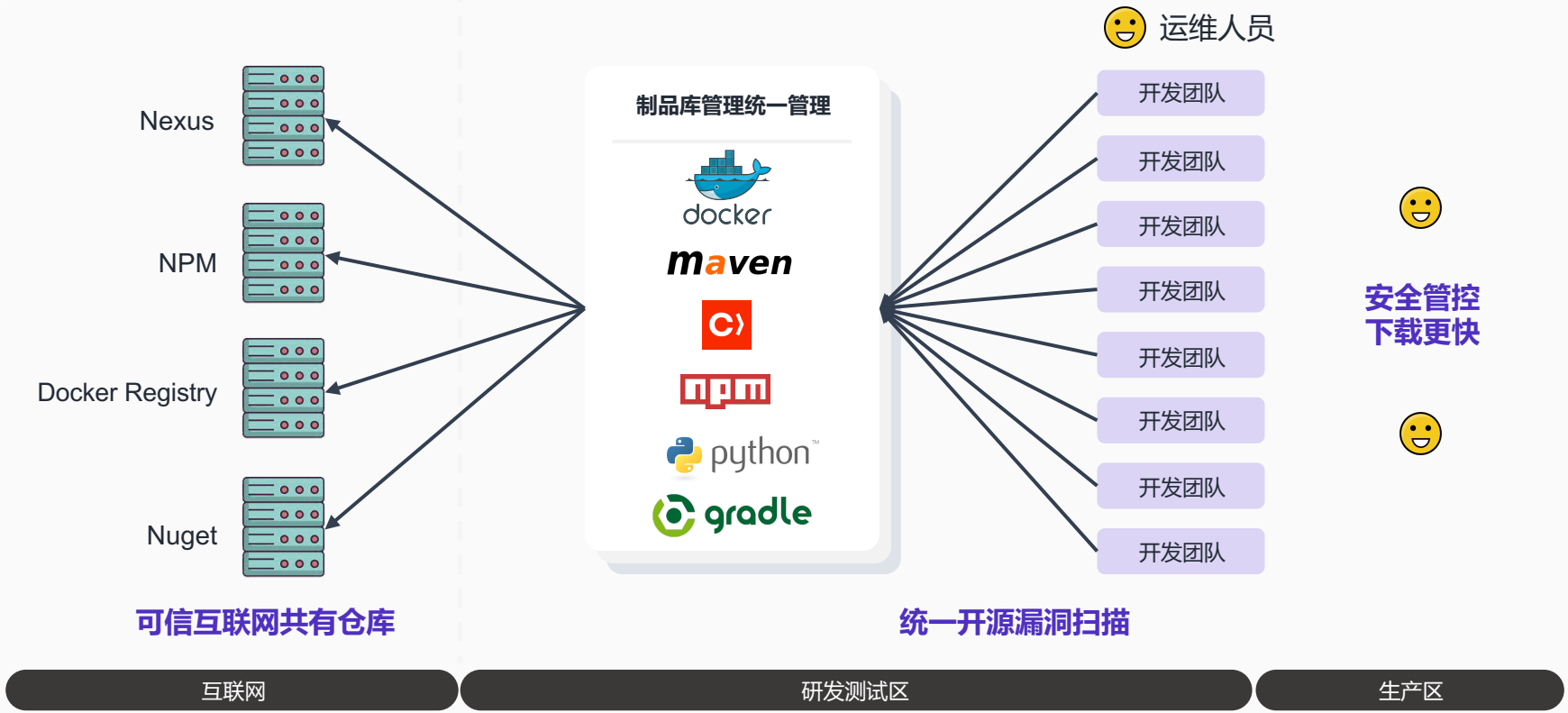
全球二进制依赖管理工具使用情况



```
➜ maven-example git:(master) ✗ mvn dependency:list
[INFO] Scanning for projects...
[INFO] ------------------------------------------------------------------------
[INFO] Reactor Build Order:
[INFO]
[INFO] Simple Multi Modules Build test                                    [pom]
[INFO] Multi 1                                                            [jar]
[INFO] Multi 2                                                            [jar]
[INFO] Multi 3                                                            [war]
[INFO]
[INFO] ----------------------< org.jfrog.test:multi >------------------------
[INFO] Building Simple Multi Modules Build test 7.0.1-SNAPSHOT            [1/4]
[INFO] --------------------------------[ pom ]---------------------------------
[INFO]
[INFO] --- maven-dependency-plugin:2.8:list (default-cli) @ multi ---
[INFO]
[INFO] The following files have been resolved:
[INFO]    junit:junit:jar:3.8.1:test
[INFO]
[INFO]
[INFO] ----------------------< org.jfrog.test:multi1 >-----------------------
[INFO] Building Multi 1 7.0.1-SNAPSHOT                                    [2/4]
[INFO] --------------------------------[ jar ]---------------------------------
[INFO]
[INFO] --- maven-dependency-plugin:2.8:list (default-cli) @ multi1 ---
[INFO]
[INFO] The following files have been resolved:
[INFO]    org.springframework:spring-beans:jar:2.5.6:compile
[INFO]    commons-logging:commons-logging:jar:1.1.1:compile
[INFO]    commons-io:commons-io:jar:1.4:compile
[INFO]    aopalliance:aopalliance:jar:1.0:compile
[INFO]    javax.servlet.jsp:jsp-api:jar:2.1:compile
[INFO]    org.apache.commons:commons-email:jar:1.1:compile
[INFO]    org.testng:testng:jar:jdk15:5.9:test
[INFO]    junit:junit:jar:3.8.1:test
[INFO]    javax.activation:activation:jar:1.1:compile
[INFO]    org.codehaus.plexus:plexus-utils:jar:1.5.1:compile
```

```
➜ npm-example node test.js
could not load livereload-js@^2.3.0 error = socket hang up
could not load typescript@^3.3.3 error = socket hang up
could not load urix@^0.1.0 status = 404
could not load to-regex-range@^2.1.0 error = socket hang up
could not load pseudomap@^1.0.2 error = socket hang up
[ 'grunt@1.2.1',
  'grunt-legacy-log@2.0.0',
  'grunt-known-options@1.1.1',
  'findup-sync@0.3.0',
  'grunt-cli@1.3.2',
  'eventemitter2@0.4.14',
  'dateformat@3.0.3',
  'glob@7.1.6',
  'grunt-legacy-util@1.1.1',
  'exit@0.1.2',
  'iconv-lite@0.4.24',
  'js-yaml@3.14.0',
  'minimatch@3.0.4',
  'rimraf@3.0.2',
  'mkdirp@1.0.4',
  'eslint-config-grunt@1.0.1',
  'difflet@1.0.1',
  'grunt-contrib-nodeunit@2.1.0',
  'grunt-contrib-watch@1.1.0',
  'grunt-eslint@18.1.0',
  'temporary@0.0.8',
  'colors@1.1.2',
  'grunt-legacy-log-utils@2.0.1',
  'lodash@4.17.19',
  'glob@5.0.15',
  'nopt@3.0.6',
  'through2@2.0.5',
```

单一可信源


运维人员
Nexus
NPM
Docker Registry
Nuget
制品库管理统一管理
docker
maven
npm
python
gradle
开发团队
开发团队
开发团队
开发团队
开发团队
开发团队
开发团队
安全管控
下载更快
可信互联网共有仓库
统一开源漏洞扫描
互联网
研发测试区
生产区

解决方案案例 - 开源治理方案及路线图

监管阶段

1、启用禁用策略
2、设置全局级、应用级白名单，例外禁用
3、制定组织级开源治理方案

监控阶段

1、开源软件摸查，出整体开源软件漏洞报告
2、建立基线库的机制
3、建立监管机制，即开源软件禁用策略

持续优化治理方案

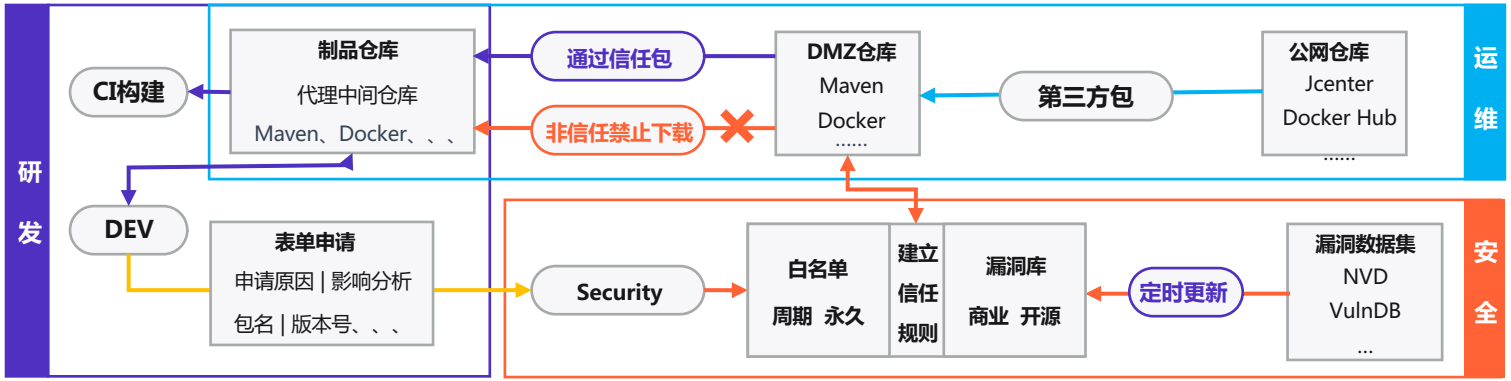
缩减漏洞白名单范围，降低安全风险

初步治理

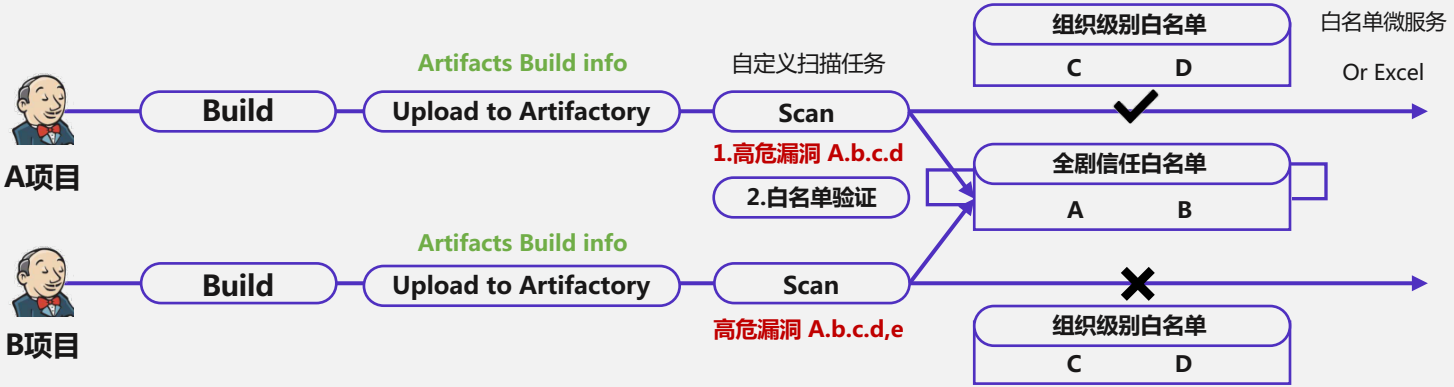
1、按项目接入制品库，分步搭建开源软件基线库
2、出接入报告，不启用禁用策略

第三方组件使用管控

全局管控



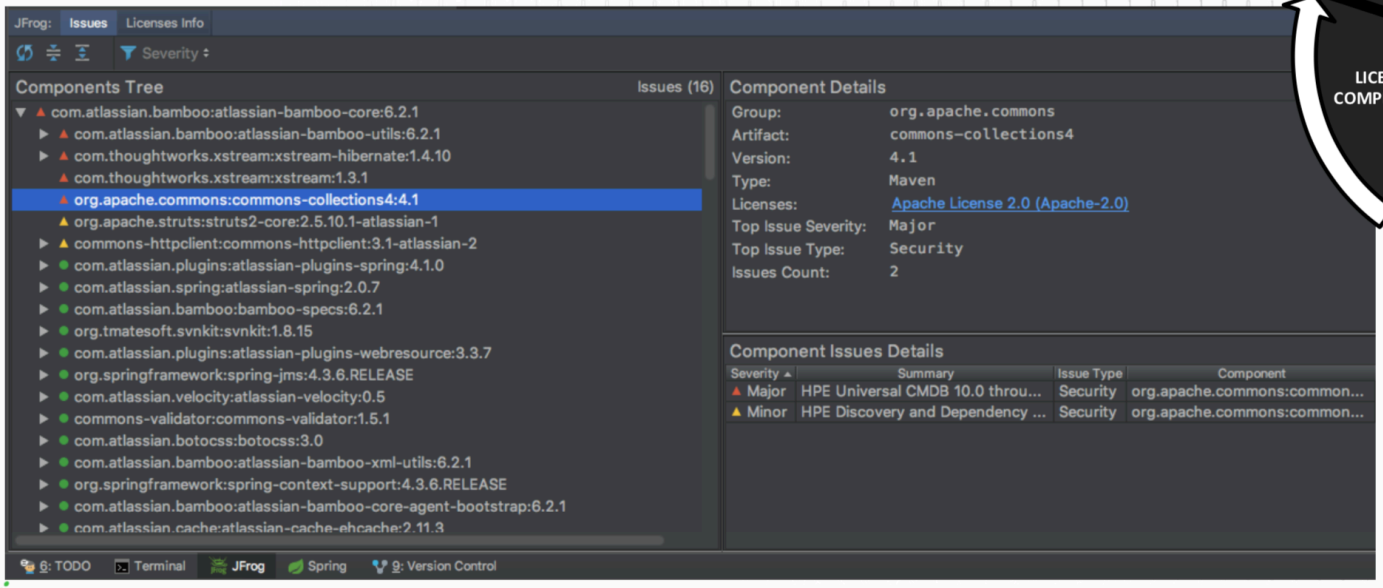
基于项目细粒度管控

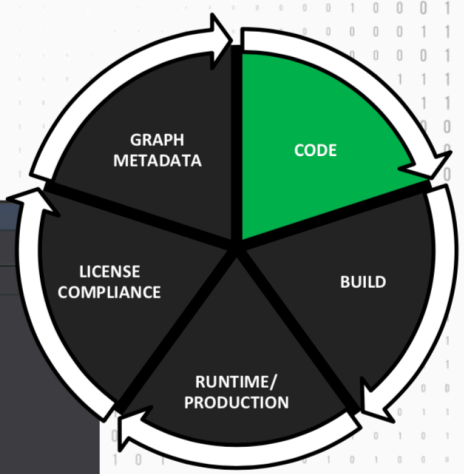


组件 & 漏洞数据源

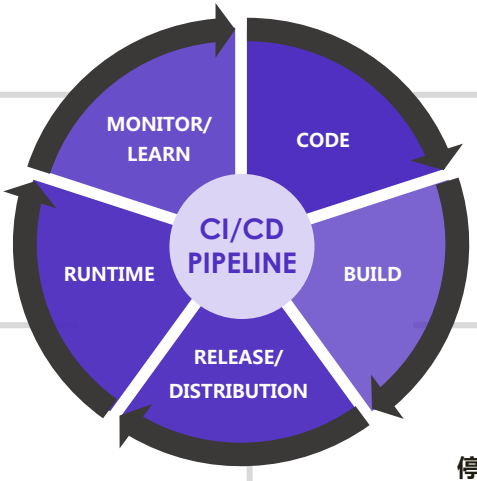
技术栈	组件信息源	漏洞信息源
Java	Https://jcenter.bintray.com	NVD:https://nvd.nist.gov CNVD:https://www.cnvd.org.cn/
Javascrip(Nodejs)	https://registry.npmjs.org	NVD:https://nvd.nist.gov CNVD:https://www.cnvd.org.cn/
Net(Nuget)	https://www.nuget.org	NVD:https://nvd.nist.gov CNVD:https://www.cnvd.org.cn/
Debian	Http://archive.ubuntu.com.ubuntu	Debian:https://security-tracker.debian.org/tracker Ubuntu:https://launchpad.net/ubuntu-cve-tracker
Rpm	http://mirror.centos.org/centos	https://www.redhat.com/security/data/oval/
Python(pypi)	https://pypi.python.org/pypi	NVD:https://nvd.nist.gov CNVD:https://www.cnvd.org.cn/
Ruby(gems)	https://rubygems.org/	NVD:https://nvd.nist.gov CNVD:https://www.cnvd.org.cn/

1. IDE Integration





JFrog Xray - 全生命周期保护



提供分析报告

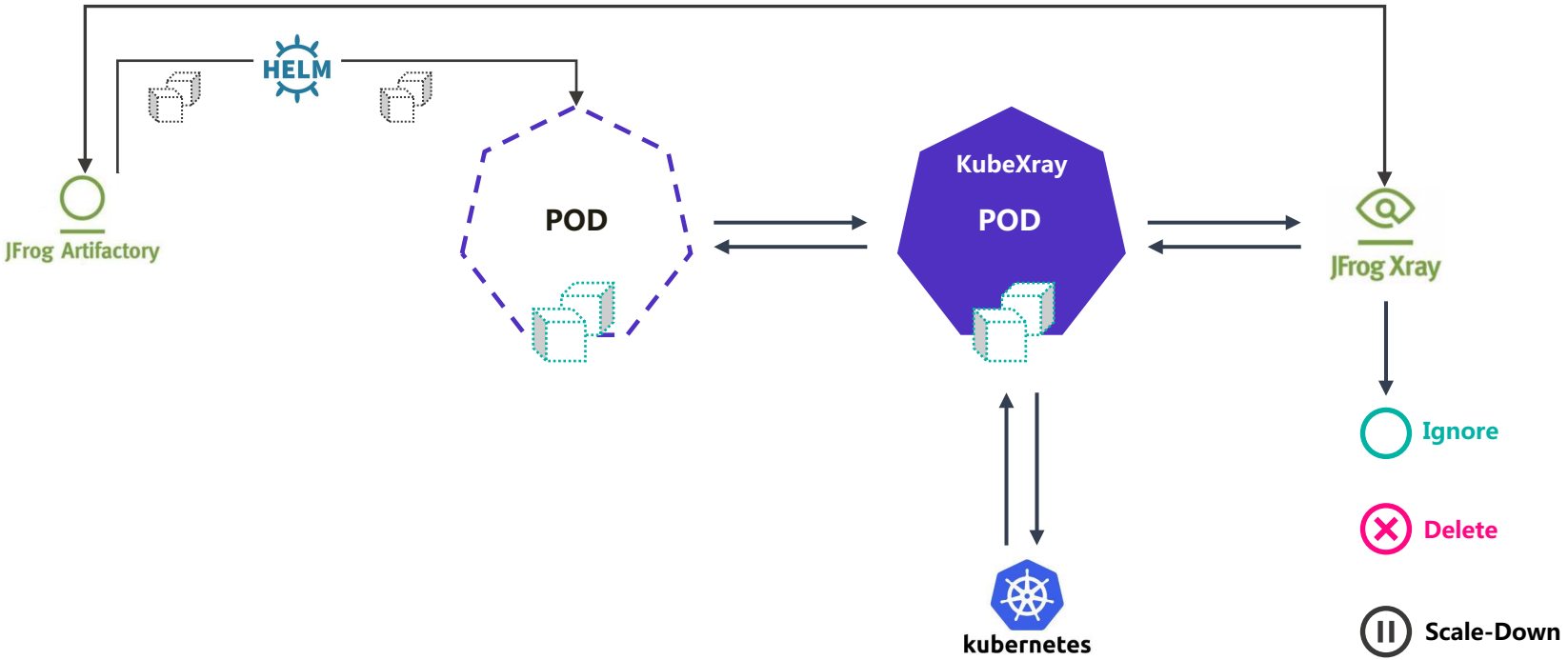
依赖组件元数据
依赖分析
集成在IDE中

生产漏洞报告
影响分析图
修复建议

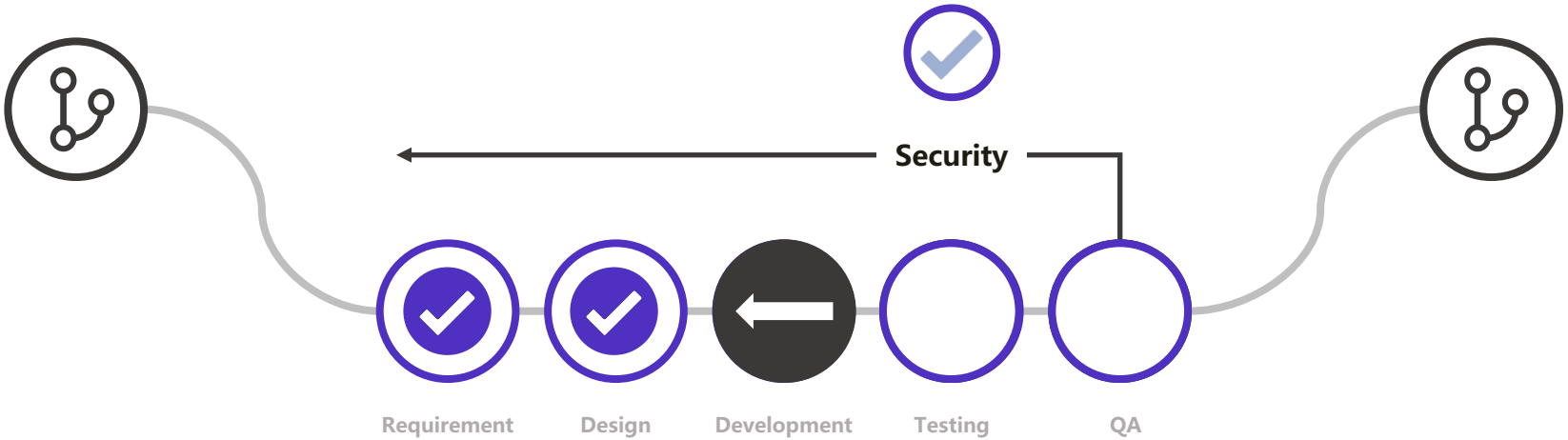
与CI集成
规则管理
停止引用有漏洞组件的构建任务
阻止下载

安全分发
阻止下载

DevSecOps - 运行时安全管控



组件 & 漏洞数据源



为什么要有开源协议？

1. 保护原作者的知识成果

防止被恶意利用。开源协议中一般都包含有免责声明，可以防止原作者承担相应风险和后果。比如你开源了一个破　解Windows秘钥的软件，而使用者却用来进行商业资料窃取，那么你是不需要为此承担责任的。

2. 保护使用者的权利

使用者可以知晓经授权和未经授权的操作。防止你使用未添加协议（可能未授权）的代码，而使原作者起诉你。

License管控的必要性

知识产权风险 | 违约风险 | 开源许可证兼容性风险 | 安全风险

随着开源软件的不断发展，社区里出现了各式各样的 License许可证，如果你使用了不合适的许可证软件，会为公司带来法律上的纠纷，同时，如果因为开源组件 License 选用不当，导致在交付的时候需要进行开源组件的替换，那随之带来的开发工作量也非常巨大。所以选择合适的许可证应该在第一时间进行。

开源软件提倡公开、自由与创新等开源精神，为推动软件产业的 发展起到了积极作用。但是，个人或企业在使用或引入开源软件的过 程中，将不可避免地面临知识产权上的风险。如个人或企业在使用或 引入开源软件，因为不了解知识产权风险而引起相关法律或商业争 议，将可能给个人或企业在经济或声誉等方面带来巨大的损失。

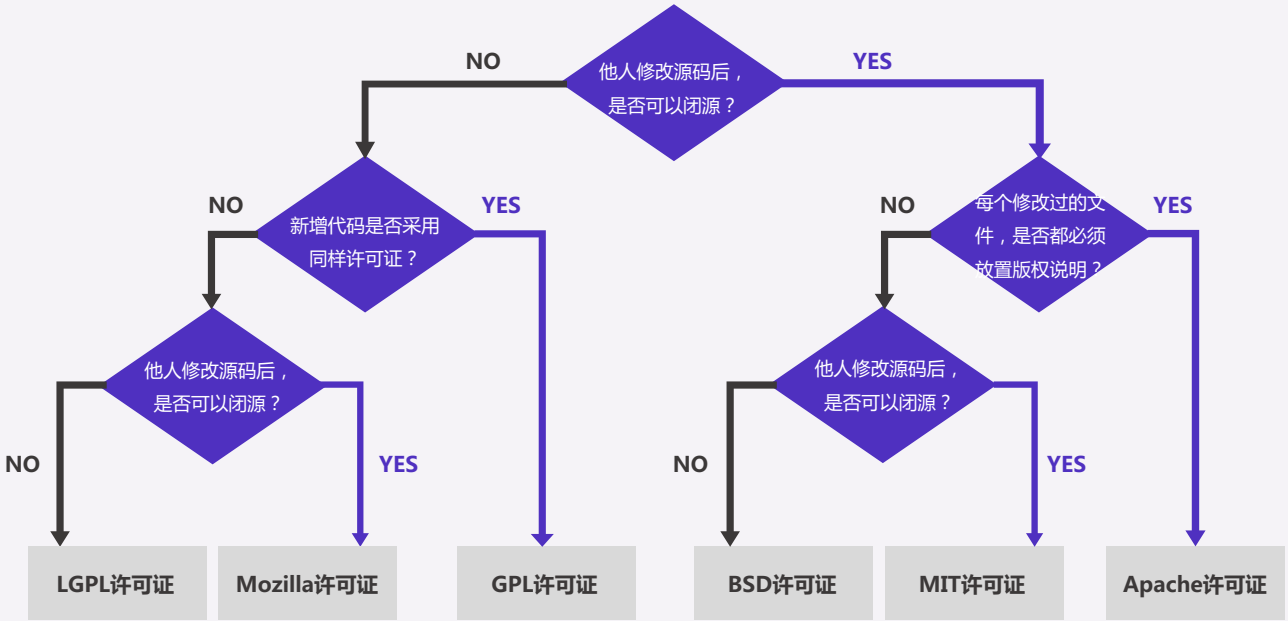
OSI开源协议查询的网站

https://opensource.org/licenses/alphabetical

常见的6种开源协议

- LGPL
- Mozilla
- GPL
- BSD
- MIT
- Apache

开源不等于免费，开源也不等于没有约束



开源治理解决方案

Open source governance solutions

统一引入管理

统一管理平台

统一审核流程

风险识别

开源许可证风险

安全风险

风险记录沟通

风险记录

沟通机制

风险处置

处置指导

漏洞修复


DATA
SECURITY
BEHAVIORAL ANALYTICS
THREAT
ANALYSIS
RISK
MANAGEMENT
ZERO TRUST
LEARNING
ATTACKS
SERVICES
BUSINESS
WEAPONIZATION
MALWARE
DIGITAL
TECHNOLOGY
DEVICES
DEVSECOPS
HUNTING
SUPPLY CHAIN
GDPR
LEARNING
INFORMATION
WORLD
APPLICATIONS
ENDPOINT SECURITY
DEFENSE
ENDPOINT
SOFTWARE
AI
IoT
NETWORK
HUNTING
CRITICAL
INTERNET
CLOUD
APPROACH
SOFTWARE
BEHAVIORAL ANALYTICS
RESPONSE
FRAUD
HUMAN PROGRESS
BEHAVIORAL ANALY
TECHNOLOGY

Q & A