
GOTC 2023
全球开源技术峰会
THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE
OPEN SOURCE, INTO THE FUTURE
「Gitee 十周年」专场
本期议题：企业软件供应链安全开源治理方案
周杰明 2023年05月28日

CONTETS

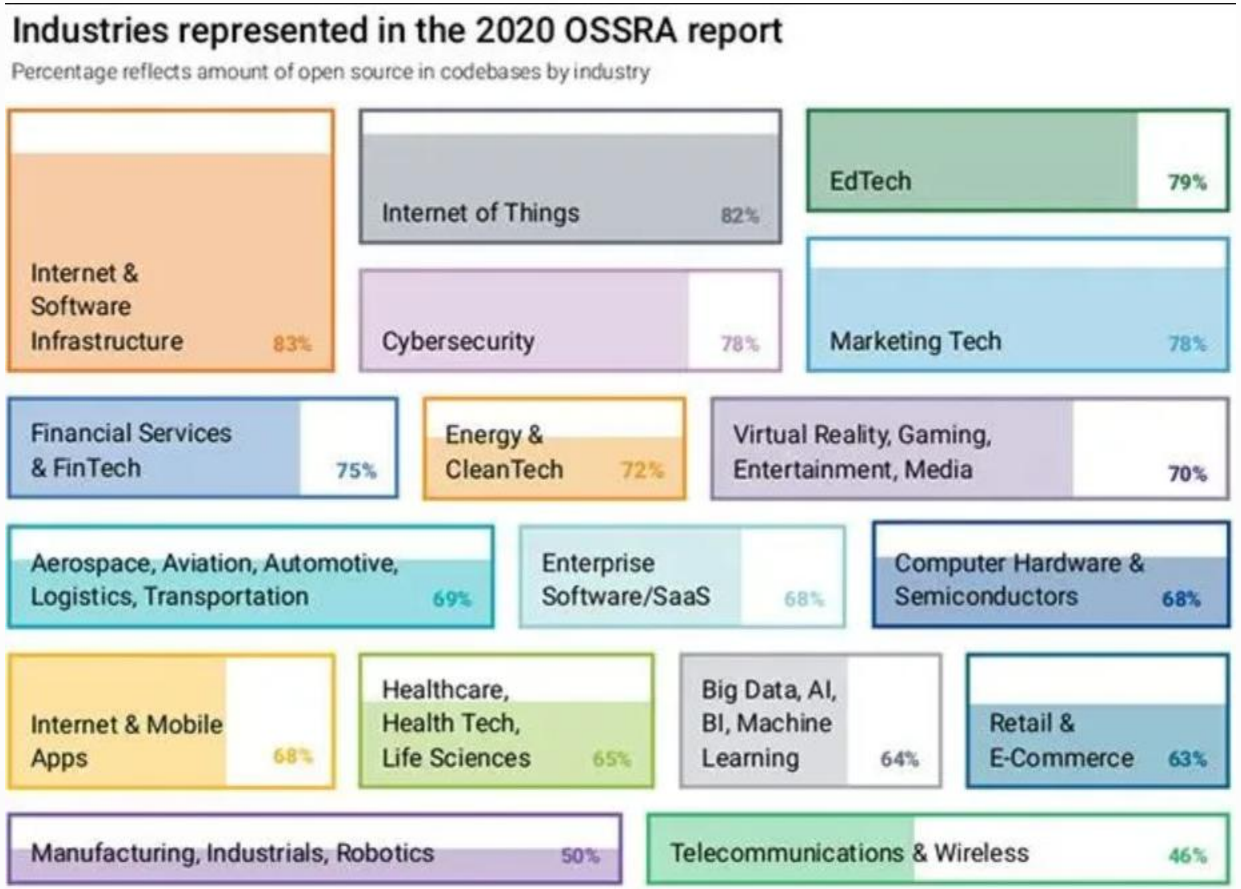
目录

CONTETS

目录

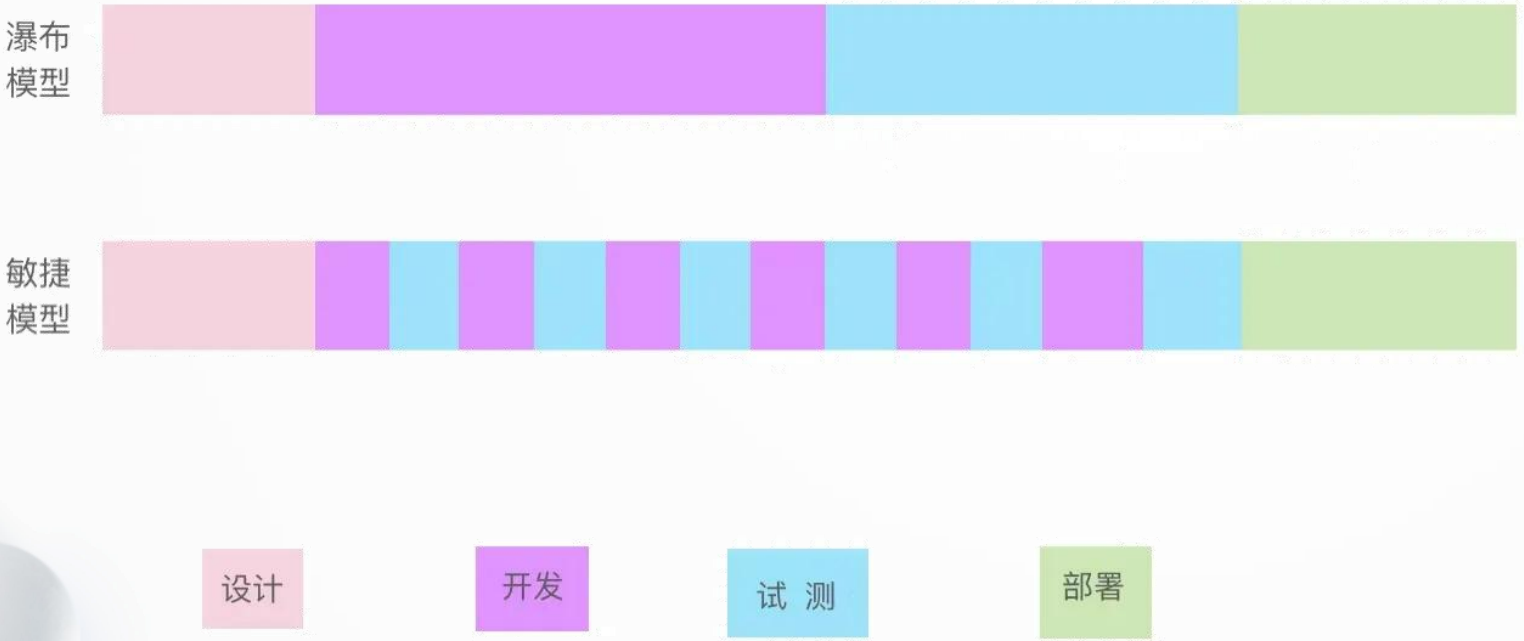
软件供应链安全背景

Synopsys 统计，在过去一年所审计的代码库中，开源组件占据了代码总量 70% 的内容。

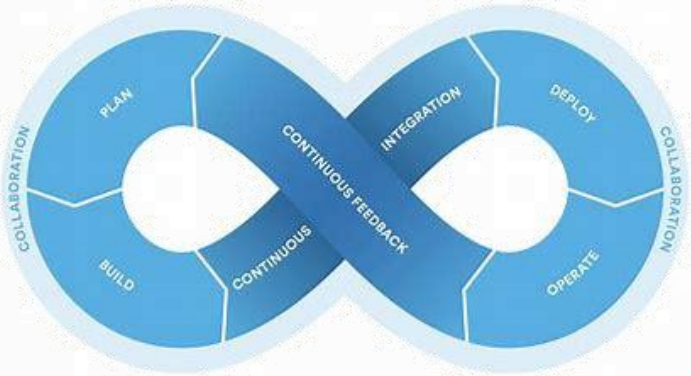


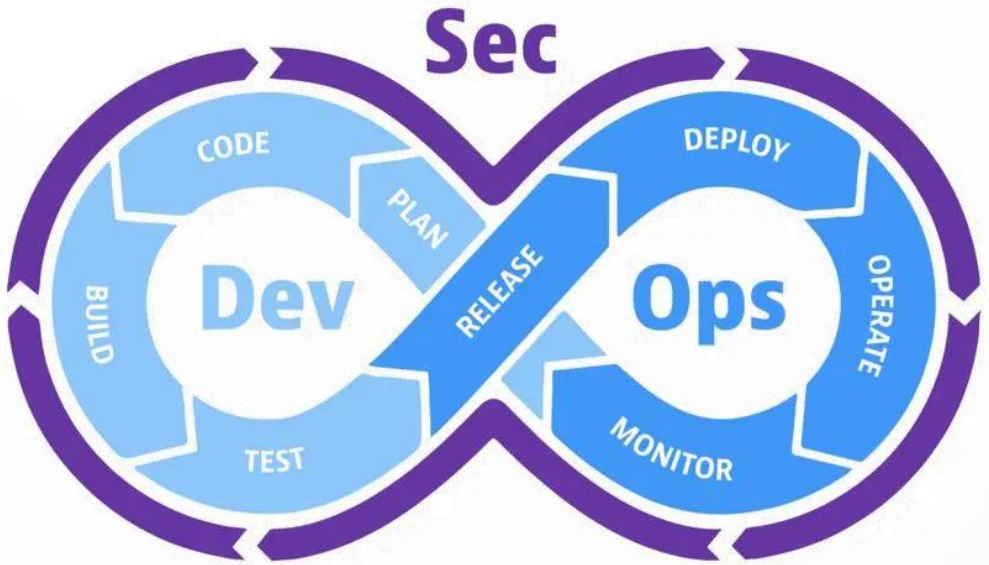
软件开发模式的演进

软件开发模式的演进

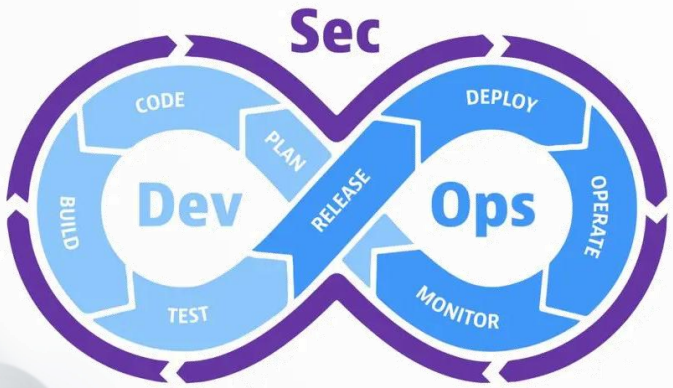


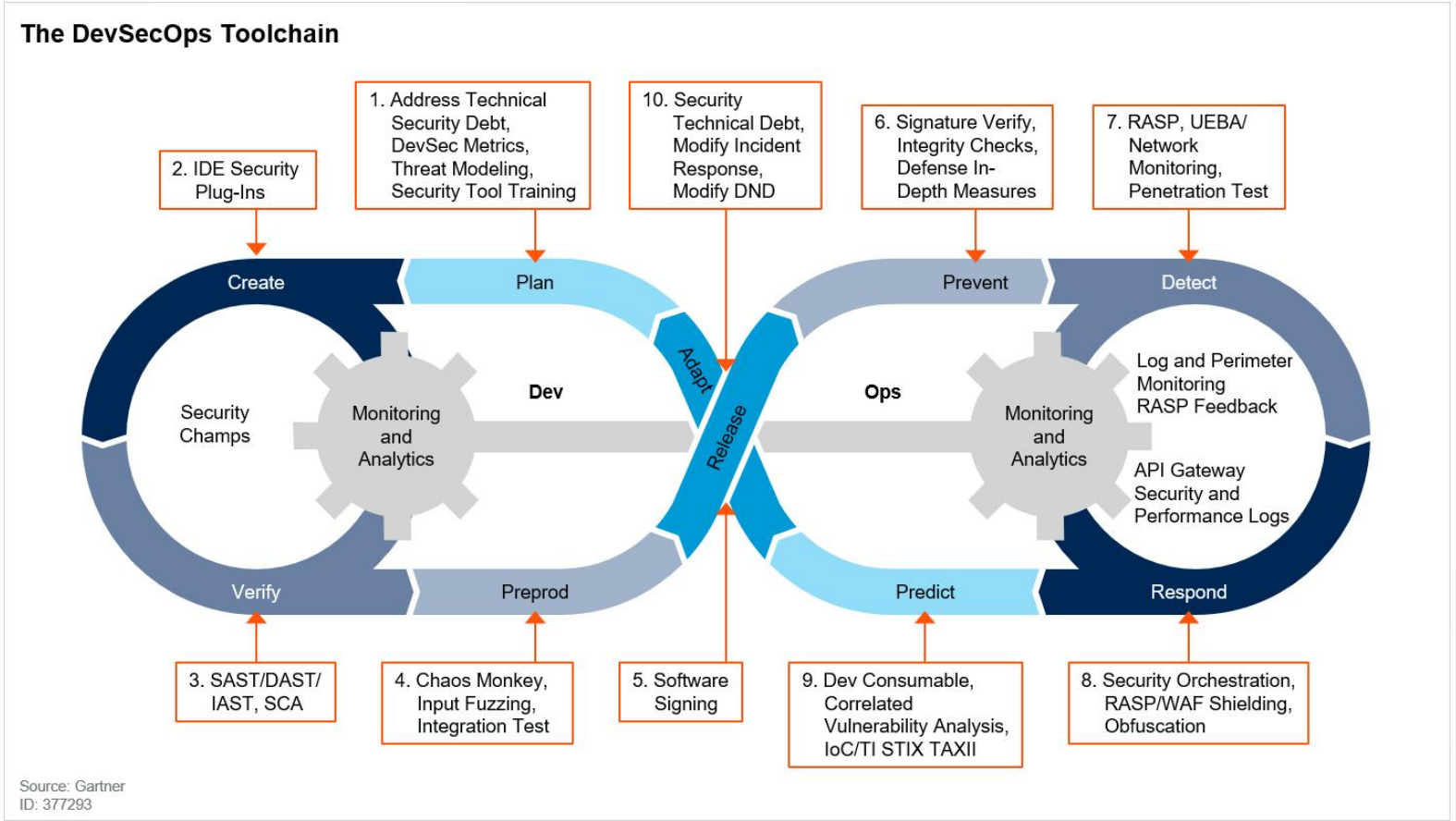
DevOps vs DevSecOps





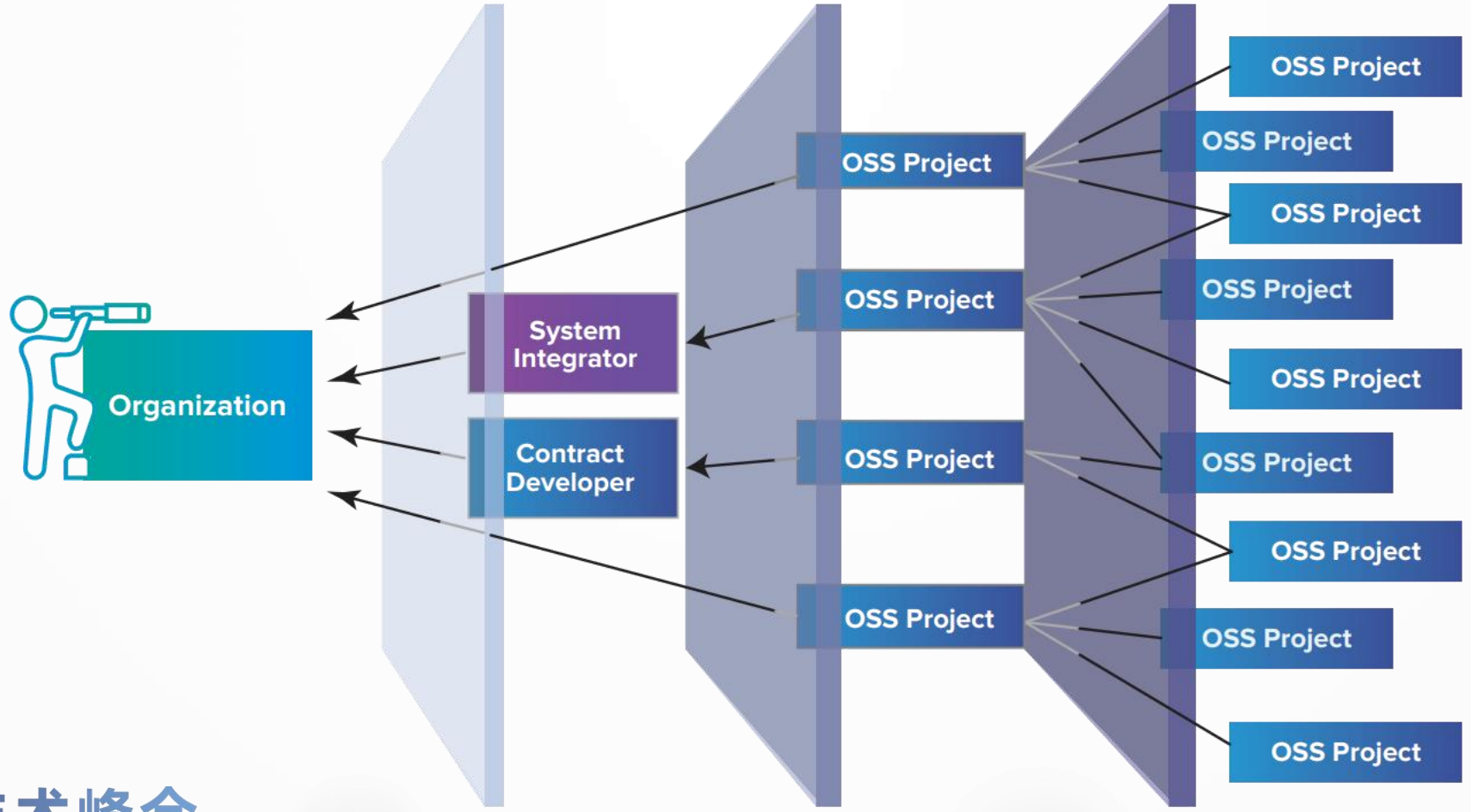
DevSecOps工具链模型





开源组件加速引入

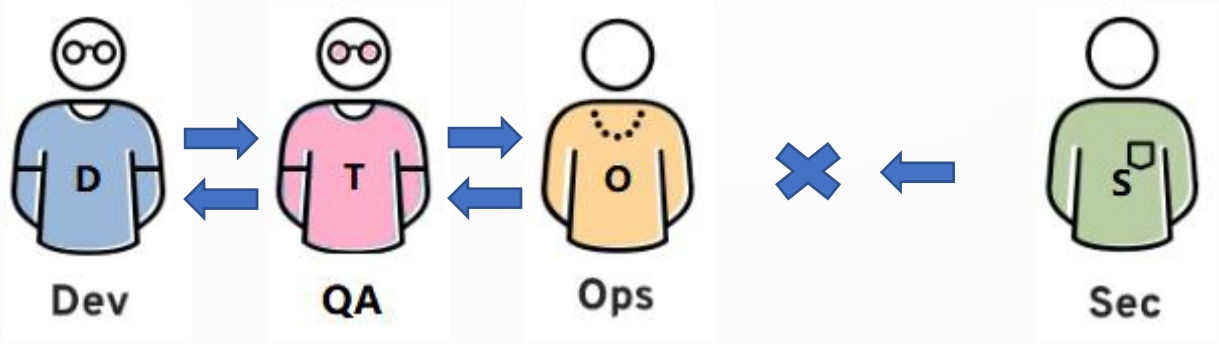
Synopsys 统计，在过去一年所审计的代码库中，开源组件占据了代码总量 70% 的内容。大量开源使用组件，研发提速，但对安全造成挑战。



软件迭代加速引发的安全问题

开发 → 测试 → 运维 → 安全

安全团队是以一种外部管理的方式参与研发团队协作。在研发团队看来，安全是麻烦。安全工作跟研发工作的目标是对立的。

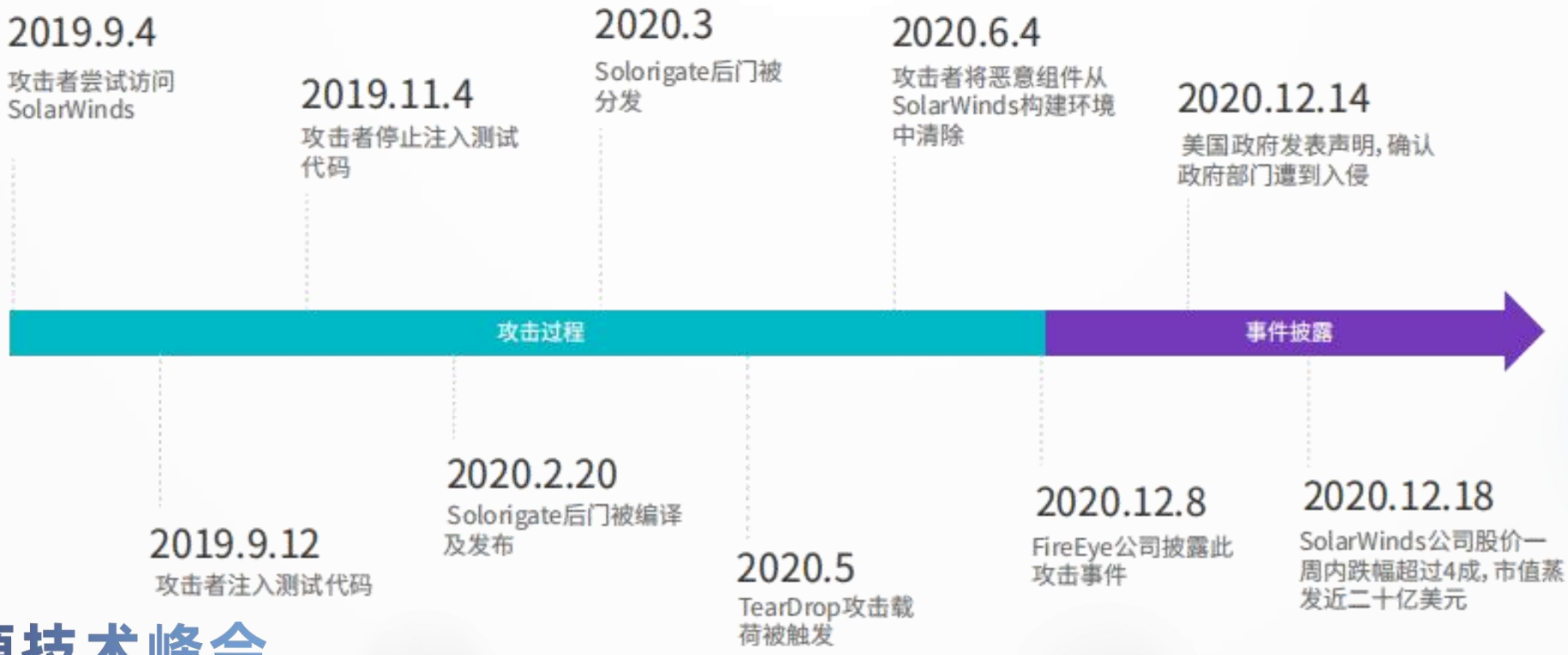


CONTETS

目录

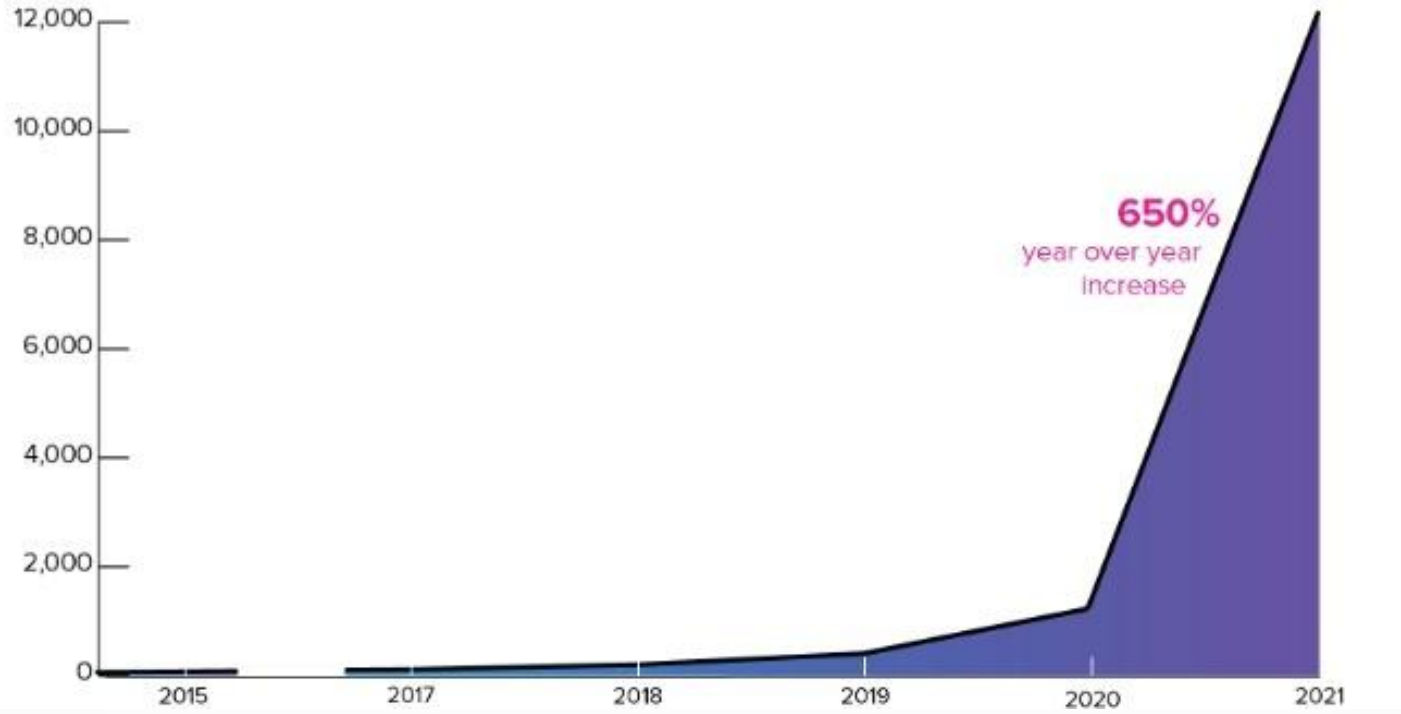
开源组件使用存在巨大漏洞风险

2020 年底，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。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。



开源攻击爆发式增长

随着开源需求的增加，开源攻击增加了650%，攻击者不再等待公开的漏洞披露来进行漏洞利用，而是主动将新漏洞注入为全球供应链提供支持的开源项目中，通过将攻击转移到“上游”，可以获得影响力和关键的时间优势，使恶意软件能够在整个供应链中传播，从而对“下游”用户进行更具扩展性的攻击。

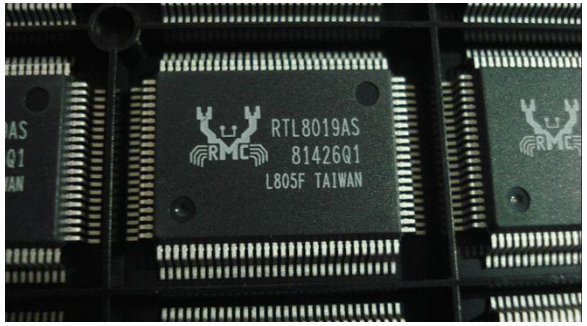


开源组件风险事故频发

软件供应链安全事件频发，“核弹级”第三方组件漏洞的影响面和危害大

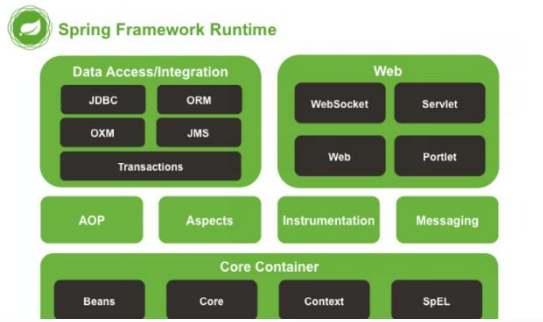
2020 年12月，美国企业和政府网络突遭“太阳风暴”攻击。黑客利用太阳风公司（SolarWinds）的网管软件漏洞，攻陷了多个美国联邦机构及财富 500 强企业网络。2020 年 12 月 13 日，美国政府确认国务院、五角大楼、国土安全部、商务部、财政部、国家核安全委员会等多个政府部门遭入侵。该事件波及全球多个国家和地区的 18000 多个用户，被认为是“史上最严重”的供应链攻击。

“太阳风暴”攻击



2021年12月，Apache开源组件Log4j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”

Apache Log4j2 漏洞



Realtek 的WiFi SDK漏洞

2021年8月，中国台湾芯片厂商Realtek 发布安全公告称在其软件开发套件和WiFi模块中发现了4个安全漏洞。、攻击者可利用该漏洞绕过身份验证，并以最高权限运行恶意代码，有效接管设备。本次暴出漏洞的芯片至少有65家供应商在使用，生产出的设备数量超过十万台。

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。

软件供应链的风险

断供风险

网络空间对抗加剧现状，会使供应链安全问题突显。

2019年美国政府把华为公司列入“实体名单”后，谷歌公司按要求暂停了与华为公司的商业往来，涉及硬件、软件和技术服务方面；

2020年8月13日起，Docker的企业版DockerEE和DockerHub禁止被美国政府列入贸易管制“实体清单”的企业使用，一批中国企业、科研院所和高校受到直接影响。

美国限制开源软件相关公司对中国的开放，以此来切断部分开源软件供应，开源软件成为贸易战的重要环节。

来源风险

软件成为新一代信息技术的灵魂，是数字经济发展的基础，是制造强国、网络强国、数字中国建设的关键支撑。

现代软件是组装的。**软件供应链污染**、供应链缺陷产生的全局网络安全问题及事件频发。

Gartner报告指出，**恶意代码注入**威胁次数的增加使得保护内部代码及外部依赖项（开源和商业软件）变得越发重要，到2025年全球45%组织机构的软件供应链将遭到攻击，这个数据将会是2021年的三倍。

软件供应链问题为未来数字化高速发展带来的阻碍和影响

合规风险

若开源软件使用者未依照相应的开源许可协议使用开源软件，将可能面临知识产权及合规风险。【出海企业风险高】

全球范围内的开源许可协议已达上百种，多种开源许可协议之间还可能存在不兼容性。2020年，98%的代码库包含开源代码，而65%的代码库存在**许可证冲突**，近四分之三的代码库包含GPL许可证冲突。违反许可证的条款造成违约行为，开源使用者很可能被开源贡献者提起**专利诉讼**并收取专利许可费。

软件供应链的新型风险

下一代软件供应链攻击（域名抢注、依赖混淆和恶意代码注入）

域名抢注：

间接攻击媒介会利用开发人员在搜索流行组件时犯下其他无害的拼写错误。

依赖混淆 ：

一种新颖的、高度针对性的攻击。媒介允许将不需要的或恶意的代码自动引入下游，而无需依赖域名抢注或品牌劫持技术。技术涉及一个坏人确定公司生产应用程序使用的专有（内部源）包的名称。

恶意源代码注入 ：

恶意源代码注入是另一种类型的攻击，与前几年相比，过去一年不太流行。此类攻击涉及将恶意源代码直接注入开源项目的存储库，并以多种方式进行。

软件供应链安全风险应对措施

供应链引入环节	软件生产环节	软件应用环节
组件来源、组件漏洞、许可证风险	开发工具、开发环境、封装工具、发布环境风险	软件升级风险、运行期间被爆风险

供应链引入阶段关键举措	软件生产阶段关键举措	软件应用阶段关键举措
• 保证存在已知风险的软件无法引入 • 此部分内容作为文字排版占位显示引入之后要记录备案形成资产信息库 • 确保引入的三方组件、基础服务无已知风险，并且要记录清单	• 确保引入的三方组件无已知风险，并且要长期动态维护清单信息 • 确保引入的三方服务无风险，并且记录清单 • 确保自研代码经过安全检查	• 持续的资产安全风险监控能力 • 具备快速止血处置的技术能力 • 具备完善的应急响应规范，经过具体的演练

当下软件供应链安全开源治理五大难点

开源组件漏洞情报

开源组件应急响应

开源组件漏洞的验证

开源组件是否被篡改的检测

基础环境内开源软件的分析

CONTETS

目录

Gitee 软件供应链安全及开源治理建设思路

研发流程

将开源技术风险检查嵌入到整个研发流程,风险左移,提质增效

管理体系

以企业为单位,构建并完善整个开源技术管理体系,多部门办同管理

可信组件库

引入可信组件库,能够实现安全漏洞、开源合规、供应链断供等核心风险的管控

标准规范

统一企业内部开源技术治理标准规范,包括代码、组件、软件、服务等不同成分

生态

积极参与源生态建设,使用开源技术并且贡献开源社区

人员

积极组织推进相关人员开源知识培训,提升开源意识,提高开源技术相关能力

可信库与规范相结合建设治理体系。

Gitee 基于源头可信的软件供应链安全解决方案

来源可信

npm docker nuget Maven Gradle GitHub

安全可信

- SCA检测
- 漏洞检测
- 后门检测
- 投毒包检测
- 病毒检测
- 组件安全指数
- 恶意代码
- 投毒风险评估
- 组件安全新闻
- 容器检测
- 源代码检测
- 组件认证
- 社区活跃度评估
- 组件漏洞情报
- 断供风险评估
- 许可证分析

Gitee可信组件库

SaaS化服务　便捷、安全

安全可信的组件镜像源

多元化交叉安全检测	安全专家定向评估	公网漏洞数据库
商业化漏洞检测工具	漏洞利用代码	NVD
开源漏洞检测工具	严重级别漏洞复现	VulnDB

Gitee 可信组件库

开源组件恶意代码分析

开源组件合规性分析

开源组件漏洞分析

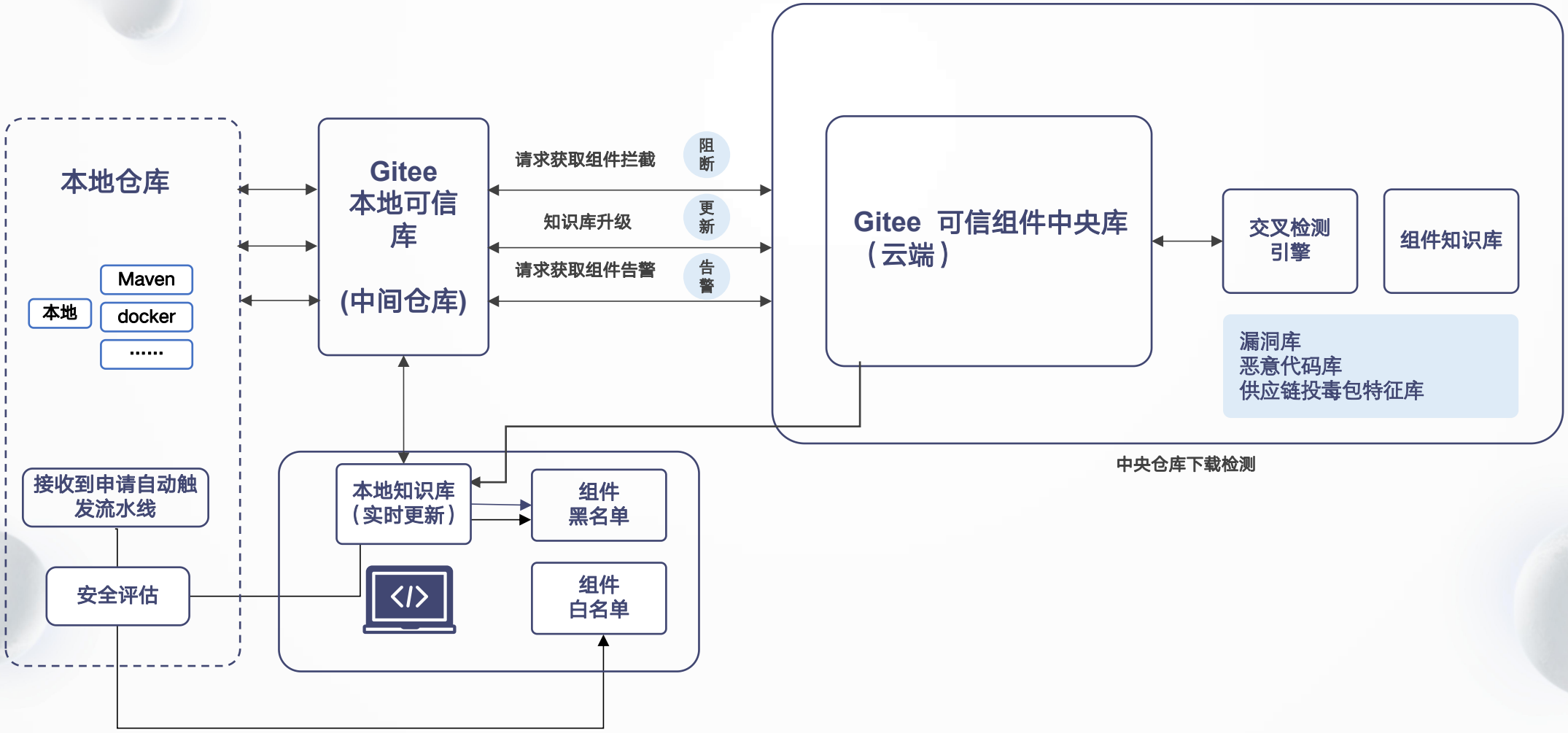
组件安全性评分

安全专家校准

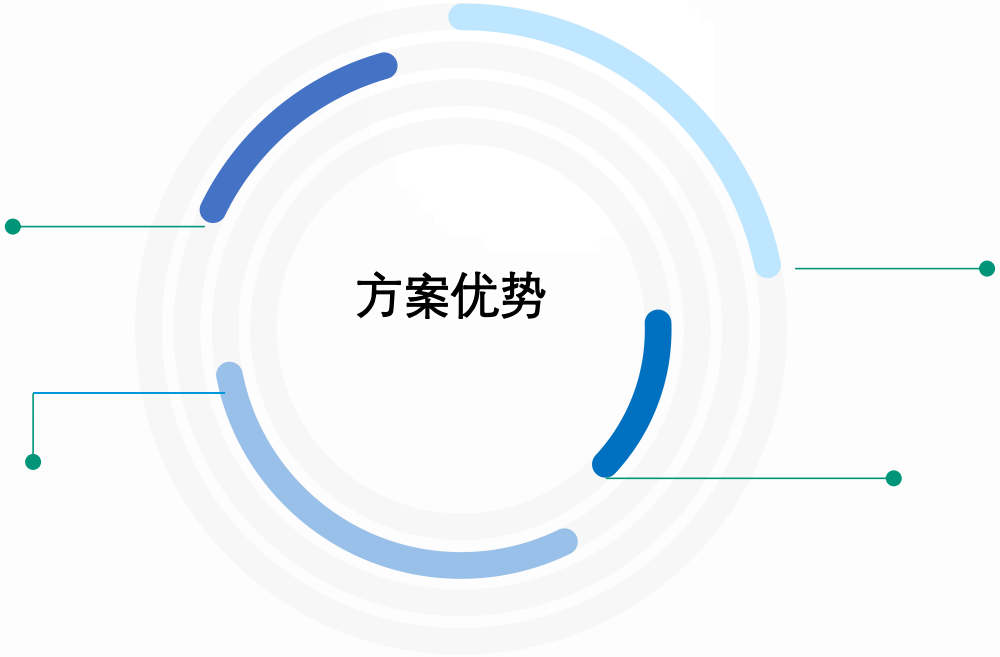
聚合

可信组件库

Gitee 可信组件库建设



可信组件库方案优势



开源组件可信入口

通过开源中国认证的可信安全开源组件库，对开源组件进行**安全引入**。

支持组件比对

从组件的引入环节入手，发现是否存在与安全可信库内不一致的被篡改混入恶意代码的外部引入组件。

降低第三方组件风险

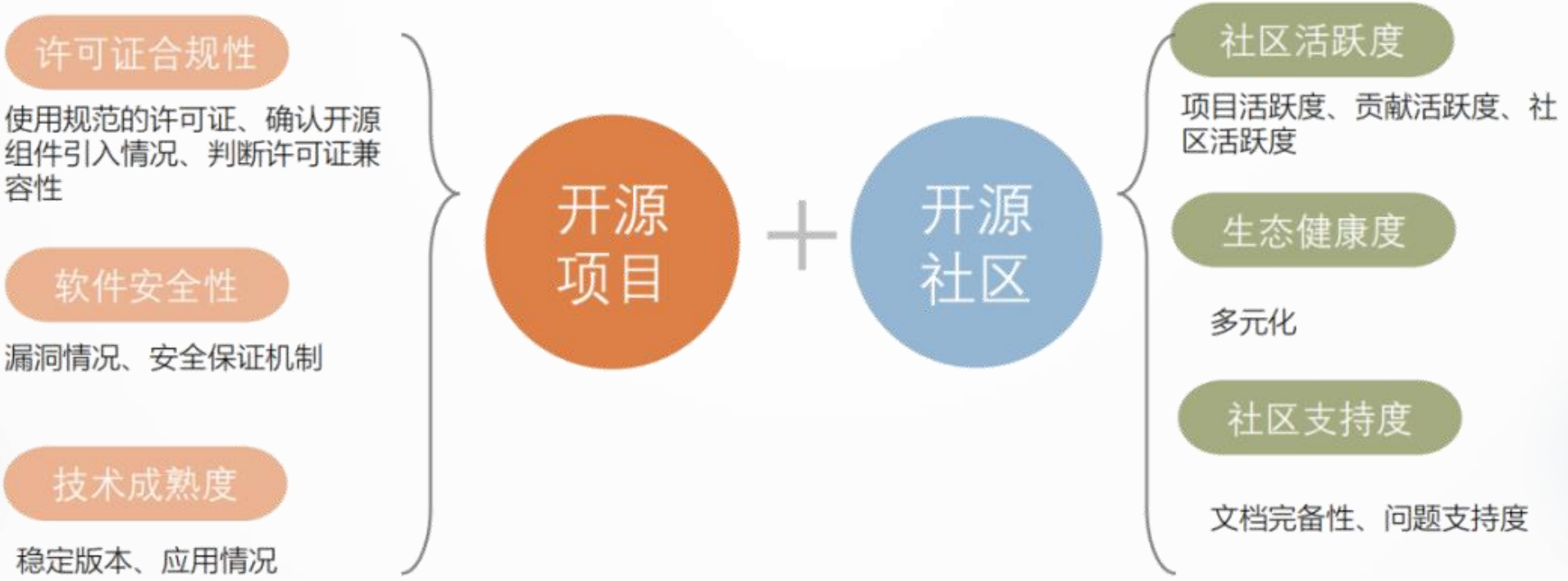
通过开源组件的可信数据库，提升组件检出率，降低组件漏洞误报率。规避或提示含有风险的组件。

大幅降低维护成本

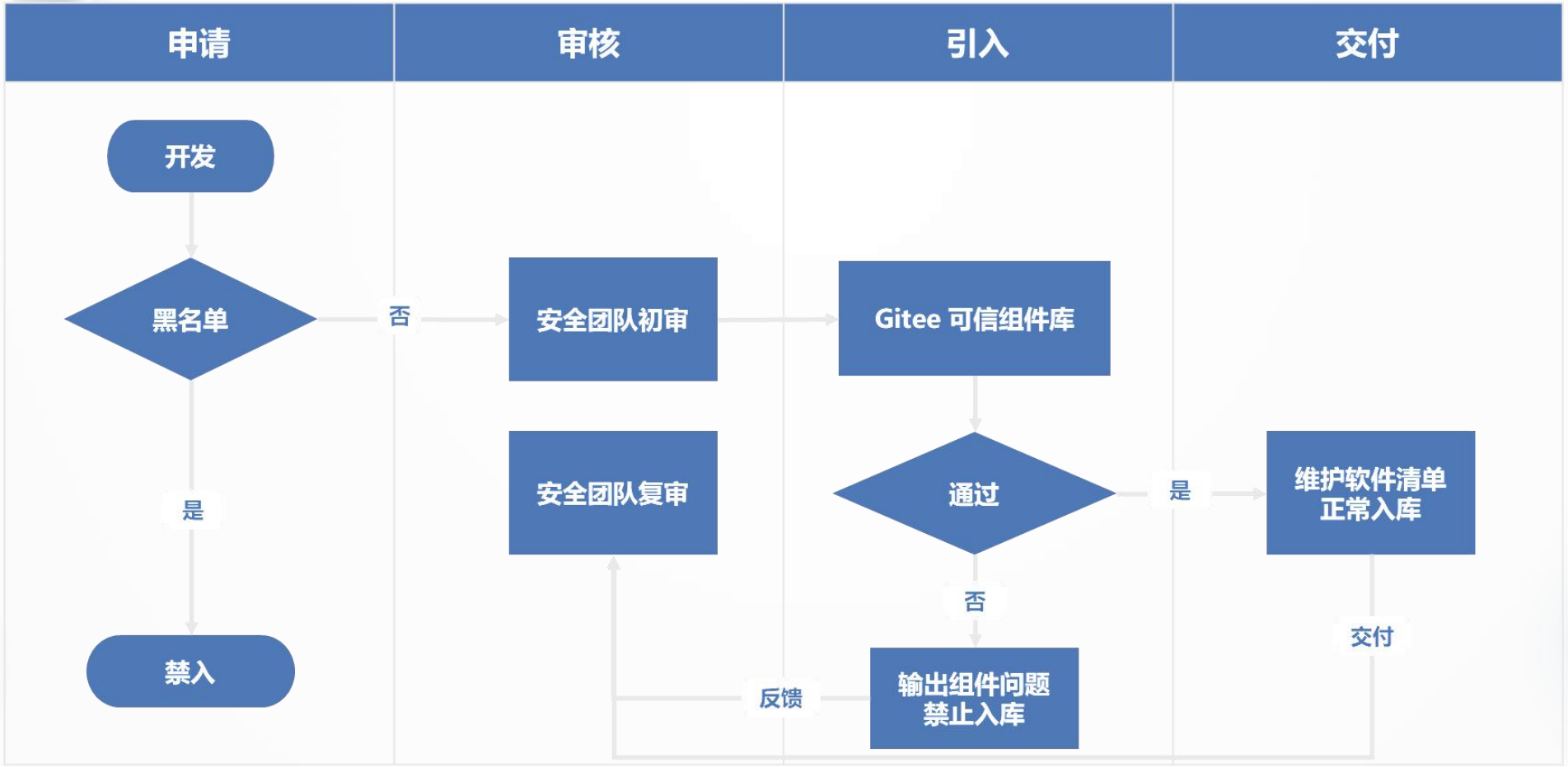
无需关心因SCA工具引起的组件误、漏报问题，以及组件新发漏洞的管理问题。大幅减少组件库的维护成本。

开源软件的引入管理

评估对象为社区版的开源项目。重点考察开源项目在许可证合规性、软件安全性、软件活跃度、技术成熟度、服务支持力和软件兼容性六个方面的能力，全面衡量社区版开源项目的健康程度，为开源项目使用方提供选型的参考依据。

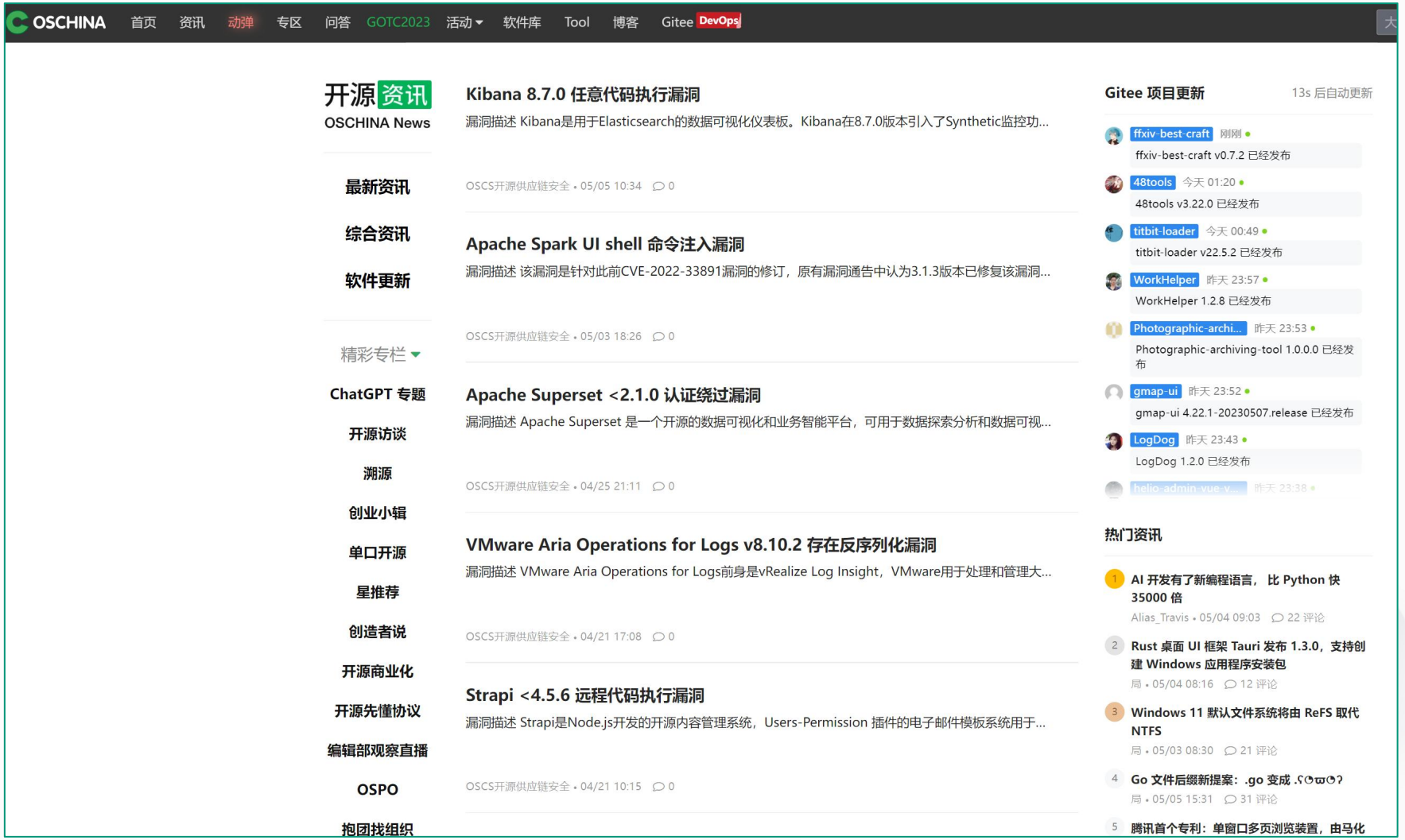


开源软件的引入管理方案



开源威胁情报及漏洞预警

针对今后随时可能爆发的开源组件漏洞，实行实时的漏洞预警推送服务。根据漏洞影响范围，可利用难度等维度，设定了不同的灾害等级。根据不同的灾害等级提供应急预案。



总结

源头把关

可信组件库统一管理，并引入安全审查机制，保证进入组织的开源私服仓库的开源组件，通过了安全审查并可信。 组件为通过安全认证的有相应标记，无安全认证的进行相应的风险提示（如安全风险、无人维护风险、断供风险等）。

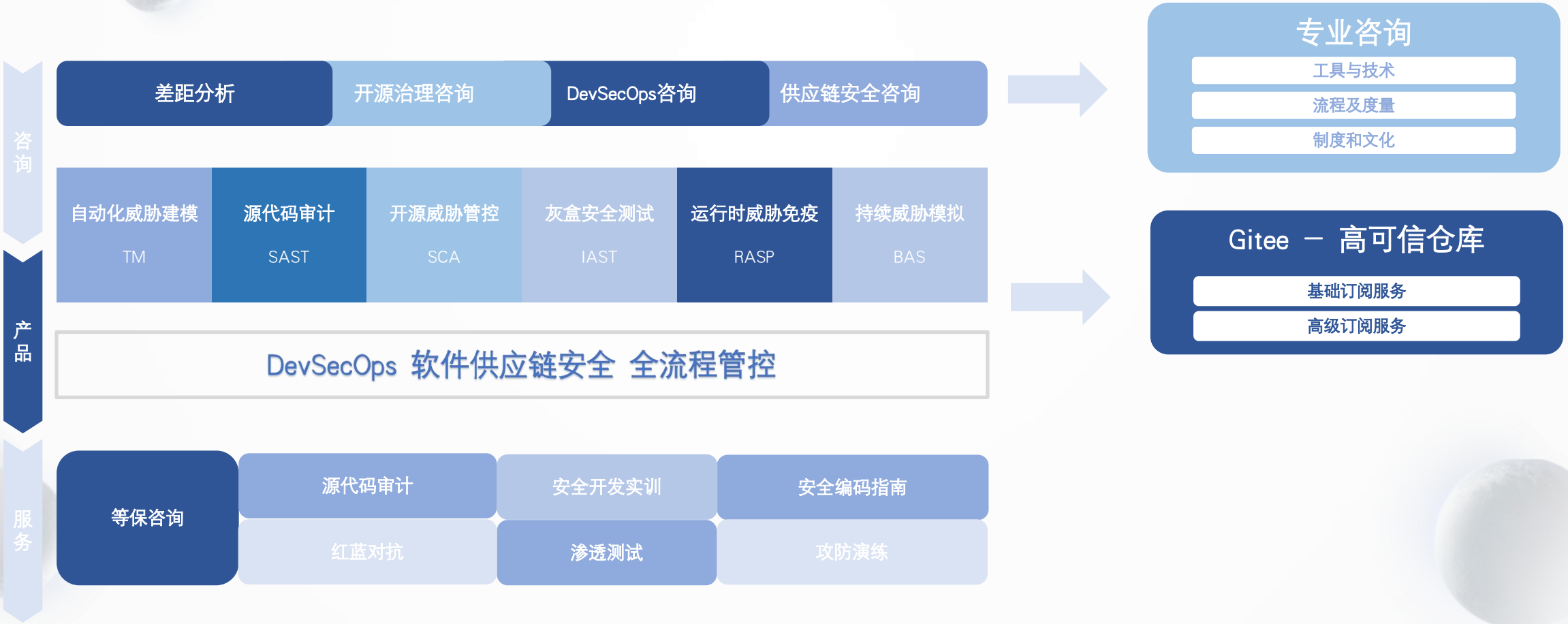
监控预警

为应对今后随时可能爆发的开源组件漏洞，实行实时的漏洞预警推送服务。并根据漏洞影响范围，可利用难度等维度，设定灾害等级。根据不同的灾害等级为企业提供相应的安全服务。让客户实时掌握自身应用程序的健康状态。

持续运营

随着突发漏洞产生调整，因此通过SBOM持续为每个应用程序构建详细的软件物料清单，全面洞察每个应用软件的组件情况，并支持根据SBOM清单第一时间采用特定预案，第一时间对相关漏洞开展修复工作。

咨询→服务→产品


咨询
差距分析
开源治理咨询
DevSecOps咨询
供应链安全咨询
产品
自动化威胁建模
TM
源代码审计
SAST
开源威胁管控
SCA
灰盒安全测试
IAST
运行时威胁免疫
RASP
持续威胁模拟
BAS
DevSecOps 软件供应链安全 全流程管控
服务
等保咨询
源代码审计
安全开发实训
安全编码指南
红蓝对抗
渗透测试
攻防演练
专业咨询
工具与技术
流程及度量
制度和文化
Gitee — 高可信仓库
基础订阅服务
高级订阅服务

CONTETS

目录

针对供应链安全的模型及评估体系

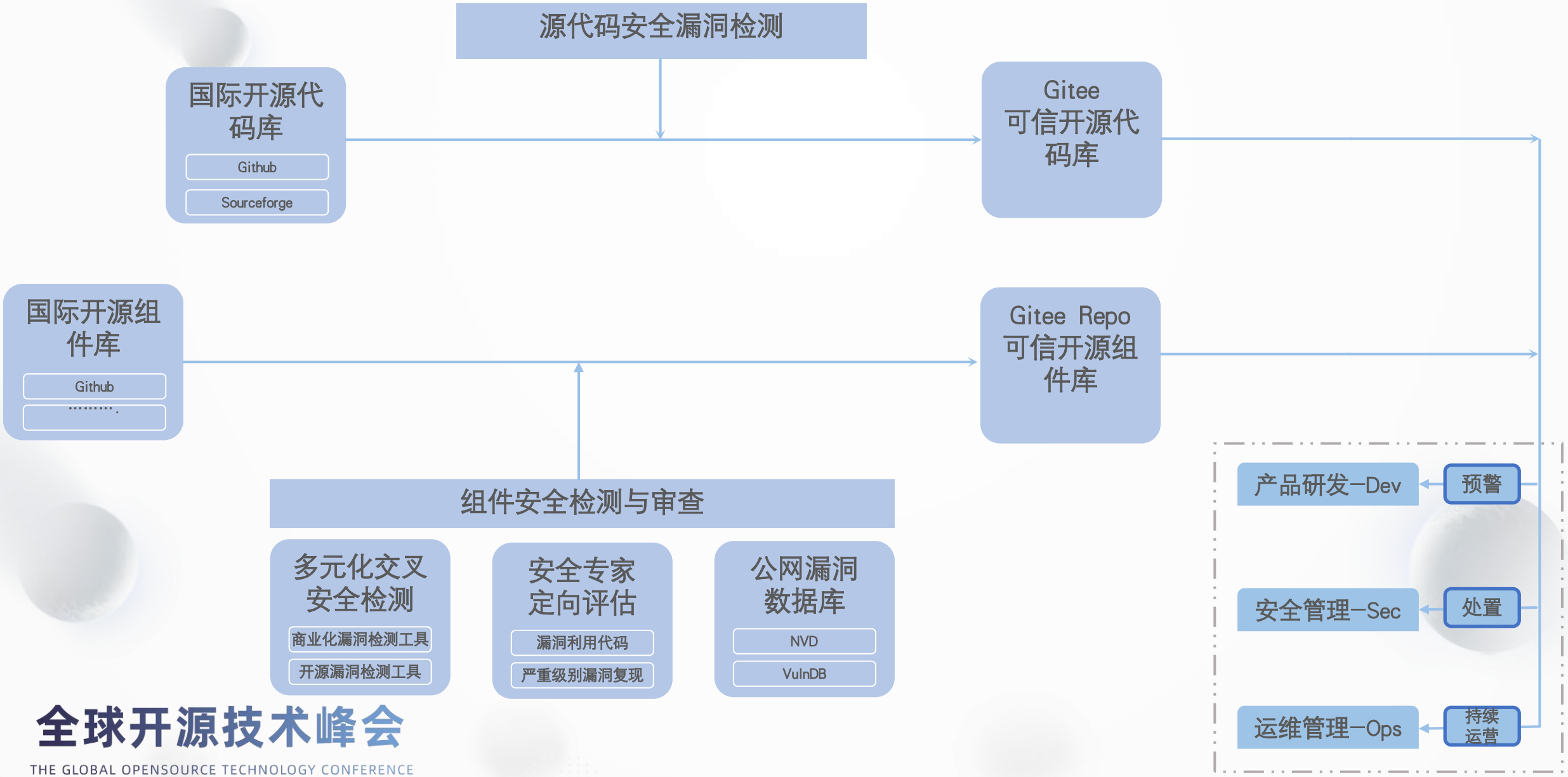
构建可信软件供应链模型

对软件供应商安全开发活动，软件成分分析，安全风险监控，安全管理和安全制度规范管理进行综合评估，在整个业务闭环中建立组件的准入登记机制，基于白名单机制形成可信组件库，从而提升供需关系信赖度。

构建行业级的软件供应链安全评估体系

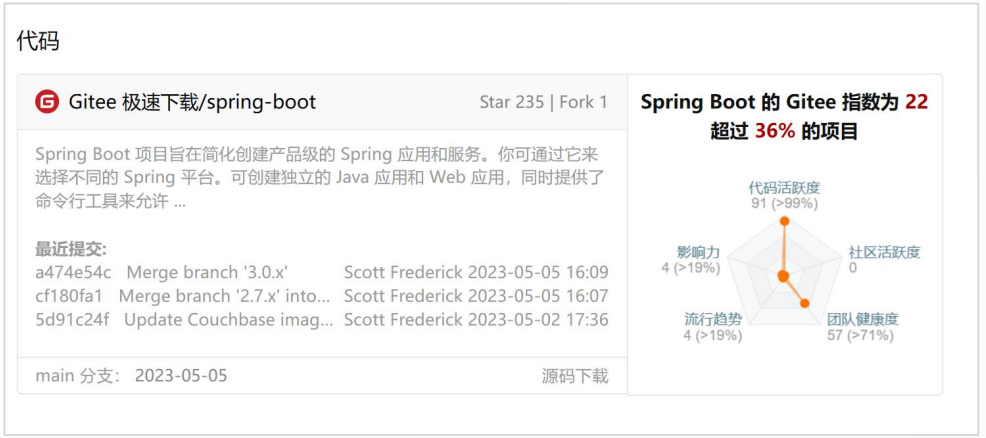
以软件供应链安全国家、行业标准为整体框架和评估业务指导，结合行业技术栈特色，在开源软件的评估过程中进一步完善评估业务规范，相辅相成输出行业级的软件供应链评估体系。

建设我国可信代码库与可信组件库



开源组件指标评估及安全象限

供应商评估



开源组件的六维安全评估

开源软件安全信息


首页 资讯 动弹 专区 问答 GOTC2023 活动 软件库 Tool 博客 Gitee DevOps
开源软件
软件首页 软件分类 国产开源 开源公司 软件资讯
+ 投递软件
大家都在搜...
开源软件库 / 国产软件 / 数据库服务器 / StarRocks
StarRocks 全场景 MPP 数据库
收藏 9 评论 0 分享
纠错
授权协议: Elastic License 2.0
开源组织: 无
开发语言: Java C/C++
地 区: 国产
操作系统: Linux
投 递 者: JohnsonGinati
软件类型: 开源软件
适用人群: 未知
所属分类: 数据库相关、 数据库服务器
收录时间: 2021-12-06
0 评论
9 收藏
分享
软件首页
软件文档
官方下载
极速下载
31.0
安全指数
概览 资讯 博客 问答 安全信息
Jetty输入验证漏洞
密码学问题
Jetty是Eclipse基金会的一个自由和开源项目，是一个基于Java的Web服务器和Java Servlet容器。 Jetty在处理哈希表单张贴和更新哈希表单时，哈希生成函数中存在漏洞。攻击者可利用此漏洞通过在HTTP POST请求中发送特制的表单，造成哈希冲突，导致较高的CPU消耗。
CVE-2011-4461 MPS-2011-4130
2022-08-08 19:00
Apache Commons HttpClient Amazon FPS 输入验证错误漏洞
证书验证不恰当
HttpClient是Apache Jakarta Common下的子项目，用来提供高效的支持HTTP协议的客户端编程工具包。 Apache Commons HttpClient 3.x版本使用在Amazon Flexible Payments Service (FPS) merchant Java SDK以及其他产品中时存在漏洞，该漏洞源于在主题Common Name（CN）或X.509证书的subjectAltName字段中，程序没有对服务器主机名与域名的匹配进行校验。中间人攻击者利用该漏洞通过任意有效的证书欺骗SSL服务器。
软件作者
JohnsonGinati
运营/编辑
关注 私信 提问
文章 经验值 粉丝 关注
4 240 4 0
同类软件推荐
更多
DB3 Network 去中心化的 Firebase 替代品
DB3 Network是一款开源的去中心化的firebase替代品，在DB3 Network上面可以...
Cozo 事务型关系型数据库
Cozo 是事务型关系型数据库，使用 Datalog 作为查询语言的高性能关系型·可嵌入式图数...
GreptimeDB Rust 实现的时序数据库
GreptimeDB 是 Rust 实现的开源时序数据库，尤其关注可扩展性、分析能力和效率，专为云...
story 关系数据库
story是一个java编写并基于mysql架构的，用来学习的关系型数据库。实现了增删改查、索...
StoneDB 基于 MySQL 的开源实时 HTAP ...
StoneDB 是基于 MySQL 内核打造的开源 HTAP (Hybrid Transactional and Analytical...

开源组件安全计划


开源软件
软件首页
软件分类
国产开源
开源公司
软件资讯
+ 投递软件
大家都在搜...
安全组件计划
安全组件计划：开源软件已接入安全扫描，时刻关注安全信息
Rails 开源网络应用框架
Ruby on Rails 是一个用于开发数据库驱动的网络应用程序的完整框架。Rails 基于 MVC（模型 - 视图 - 控制器）设计模式。从视图中的 Ajax 应用，到控制器中的访问请求和反馈，到封装数据库的模型，Rails 为你提供一个纯 Ruby 的开发环境。发布网站时，你只需要一个数据库和一个网络服务器即可。
更新于 2023/05/08 12:24
OpenMLDB 面向机器学习应用的数据库
OpenMLDB 是一个面向机器学习应用提供正确、高效数据供给的开源数据库。除了超过 10 倍的机器学习数据开发效率的提升，OpenMLDB 也提供了统一的计算与存储引擎减少开发运维的复杂性与总体成本。
更新于 2023/05/08 12:23
Solana 构建可扩展的加密货币应用程序
Solana 是一个快速、安全、抗审查的区块链，提供全球采用所需的开放基础设施。专注于你的业务，而不是你的区块链基础设施。Solana 通过在网络扩展时维持一个单一的全局状态，确保生态系统项目之间的可组合性。
更新于 2023/05/08 12:22
flink Apache Flink
经典的大数据组件
更新于 2023/05/08 12:20
热门软件
GitHub - 代码托管服务平台
收藏 350 评论 73
Steam++ - Steam 工具箱
收藏 51 评论 9
Tampermonkey - Chrome 脚本扩展
收藏 25 评论 16
Element - 基于 Vue 2.0 的组件库
收藏 1679 评论 58
Scratch - 儿童编程学习平台
收藏 135 评论 3
MATLAB - 数学软件
收藏 75 评论 4
Vant - 基于 Vue 2.0 的 Mobile 组件库
收藏 815 评论 40
XMind - 思维导图软件
收藏 443 评论 16
Blender - 三维绘图及渲染软件
收藏 246 评论 5
Safari - 苹果浏览器
收藏 15 评论 8

GOTC

THANKS

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE