墨菲安全
MURPHYSEC

以开发者为核心
行业领先的软件供应链安全平台

开源许可证合规管理解决方案

2024.01

关于墨菲安全

懂企业 超十年甲方应用安全建设经验，核心团队来自百度、华为、平安、招行、贝壳；

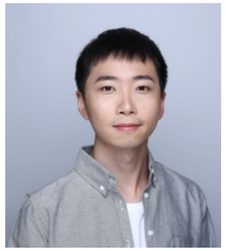
产品技术领先 顶级的漏洞研究及应用安全实践经验，创始人曾在乌云主导国内首款检测SaaS产品TangScan；

和客户一起成长 软件及应用安全重运营，墨菲安全理念是伴随客户安全业务一起成长，持续迭代创新；

核心团队

创始人&CEO 章华鹏

前百度安全架构师，乌云产品合伙人
top10白帽子，首款SaaS产品tangscan
独立发现国内外企业数百个严重漏洞

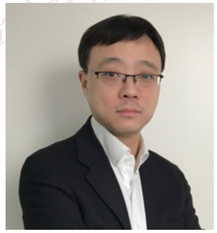


联创&实验室负责人 欧阳强斌

前百度、贝壳资深安全工程师
曾负责百度蓝军攻防团队
贝壳基础安全团队负责人

联创&工程负责人 宇佰超

前华为、贝壳工程技术专家
曾负责华为多款安全产品的研发及架构设计，贝壳零信任架构负责人



合伙人&COO 周欣

前梆梆安全COO，负责营销工作
在安全市场营销及销售方面超过二十年的丰富经验，专业的客户服务能力

联创&方案负责人 崔泷跃

前平安、招行及百度资深安全工程师
超过十年的开发安全、DevSecOps及SDL方面的落地经验

联创&产品负责人 车志远

前百度、贝壳资深安全工程师
曾负责单一企业超过50万用户的企业级安全产品的设计及落地

部分典型客户案例

墨菲安全 MURPHYSEC

互联网

Tencent 腾讯　Alibaba Group 阿里巴巴集团　Baidu 百度　美团　xiaomi　快手　京东　贝壳 让居住更美好　小红书

金融业

中国银行 BANK OF CHINA　蚂蚁集团 ANT GROUP　中国平安 PING AN 保险·银行·投资　广发银行 CHINA GUANGFA BANK　兴业证券 INDUSTRIAL SECURITIES　南京银行 BANK OF NANJING　大家保险 DAJIA BAOXIAN

运营商

中国移动 China Mobile　中国电信 CHINA TELECOM 世界触手可及　天翼云

能源及制造

国家电网 STATE GRID　中国建筑 CHINA STATE CONSTRUCTION　理想

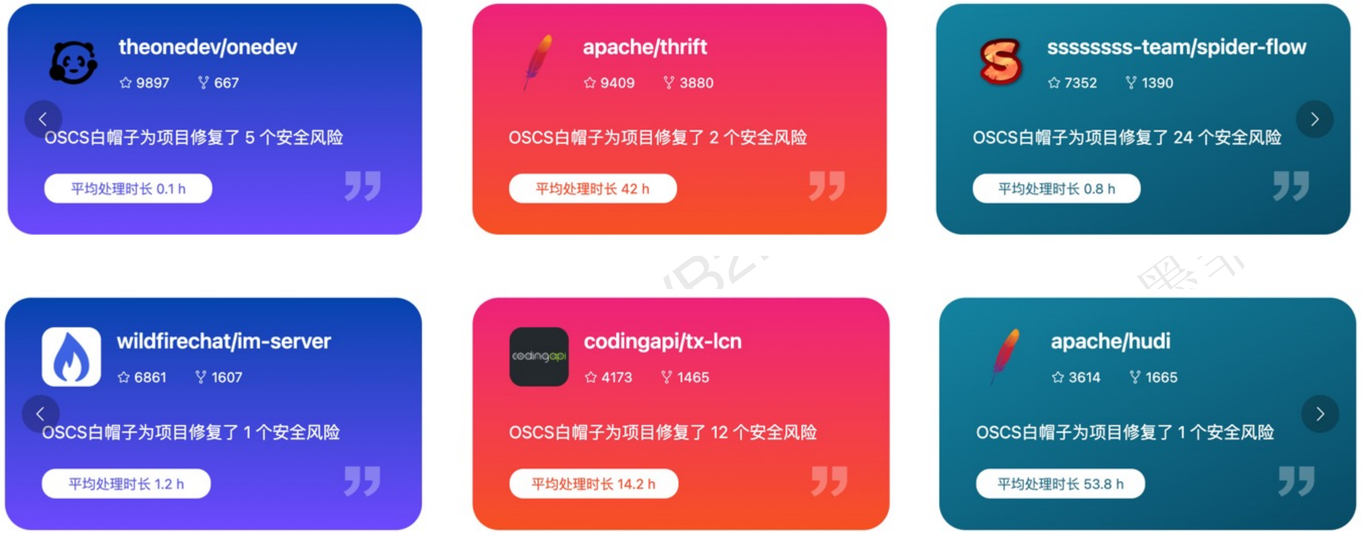
监管合作

中华人民共和国公安部 The Ministry of Public Security of the People's Republic of China　中国人民银行 THE PEOPLE'S BANK OF CHINA　CNCERT/CC 国家互联网应急中心　CAICT 中国信通院

全球首个软件供应链安全技术社区 实力验证

墨菲安全 MURPHYSEC

500+顶级开源项目通过OSCS社区一键修复安全漏洞



超过20000个开发者正在使用墨菲安全SaaS产品

36万 累计检测项目数

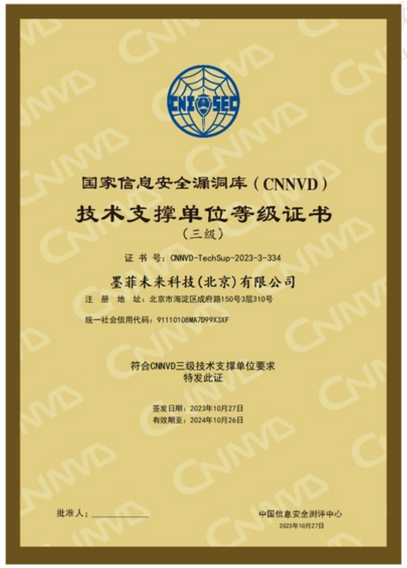
750万 累计发现漏洞数

41万 知识库覆盖漏洞数

8000万 知识库覆盖组件数

资质及荣誉

墨菲安全
MURPHYSEC



墨菲安全八大场景解决方案

墨菲安全
MURPHYSEC

开源组件安全风险治理

适用场景：因监管及安全事件，需开展开源安全/合规治理
相关监管：银保监、公安部、工信部、证监会等
产品特性：漏洞可达性分析、修复兼容性评估、网关准入准出
适用行业：金融/运营商/互联网/能源/关基/制造 等
典型客户：快手、中国移动、中国银行、中国电信、兴业证券、小红书

资产及漏洞投毒应急响应

适用场景：突发0day及投毒事件应急响应，避免勒索及数据泄露
相关监管：公安部、网信办、银保监等
产品特性：0day首发预警、投毒情报、25+独家漏洞分析字段
适用行业：互联网/金融/运营商/能源/关基 等
典型客户：蚂蚁、美团、阿里、腾讯、国家电网、理想汽车、微众银行

开源组件许可证风险治理

适用场景：企业产品出海/交付甲方/对外开源担心出现许可证合规风险
相关监管：知识产权保护法、甲方安全要求、开源社区准则
产品特性：代码片段级溯源、二进制及固件成分分析
适用行业：车企/IoT厂商/软硬件出海企业/先进制造 等
典型客户：理想、高德、小米、美团、道通科技

车企/智能制造安全及合规

适用场景：面临国内外严格的标准要求，对许可证及漏洞风险管理严格
相关监管：欧盟R155、国内车企强标、国内外知识产权保护法
产品特性：全球领先漏洞知识库、代码片段级溯源、二进制及固件分析
适用行业：智能网联车/先进制造 等
典型客户：理想、小米、道通科技

墨菲安全八大场景解决方案

墨菲安全
MURPHYSEC

商业软件供应链安全治理

适用场景：企业大量外采软件供应商漏洞及数据泄露导致企业受影响
相关监管：银保监、公安部、工信部、证监会等
产品特性：网关准入准出、商业软件二进制安全检测、软件供应商情报
适用行业：金融/运营商/能源/关基/互联网 等
典型客户：中国移动、中国银行、中国电信、兴业证券、广发银行

护网资产及风险排查

适用场景：护网前对存在安全漏洞及隐患的供应链资产排查整改
相关监管：公安部、通管局
产品特性：资产识别、0day知识库、POC、快速修复
适用行业：金融/运营商/能源/关基 等
典型客户：中国移动、天翼云、中国银行等

软件安全检测报告及SBOM

适用场景：软件厂商在投标及交付产品时需带安全检测报告及SBOM
相关监管：甲方企业安全要求
产品特性：行业认可的检测报告、SBOM导出、报告导出
适用行业：软件厂商 等
典型客户：道通科技、广州嘉为、沃丰科技

监管软件安全产品检测及认证

适用场景：作为监管及认证单位，需要自动化对产品进行检测认证
相关监管：各类国标
产品特性：简单易用、结果准确、覆盖率高、可解释性强
适用行业：监管、检测认证机构 等
典型客户：信通院、公安部、金融认证中心 等

目录

墨菲安全
MURPHYSEC

专业、专注、可靠

01 背景介绍

02 治理挑战

03 解决方案

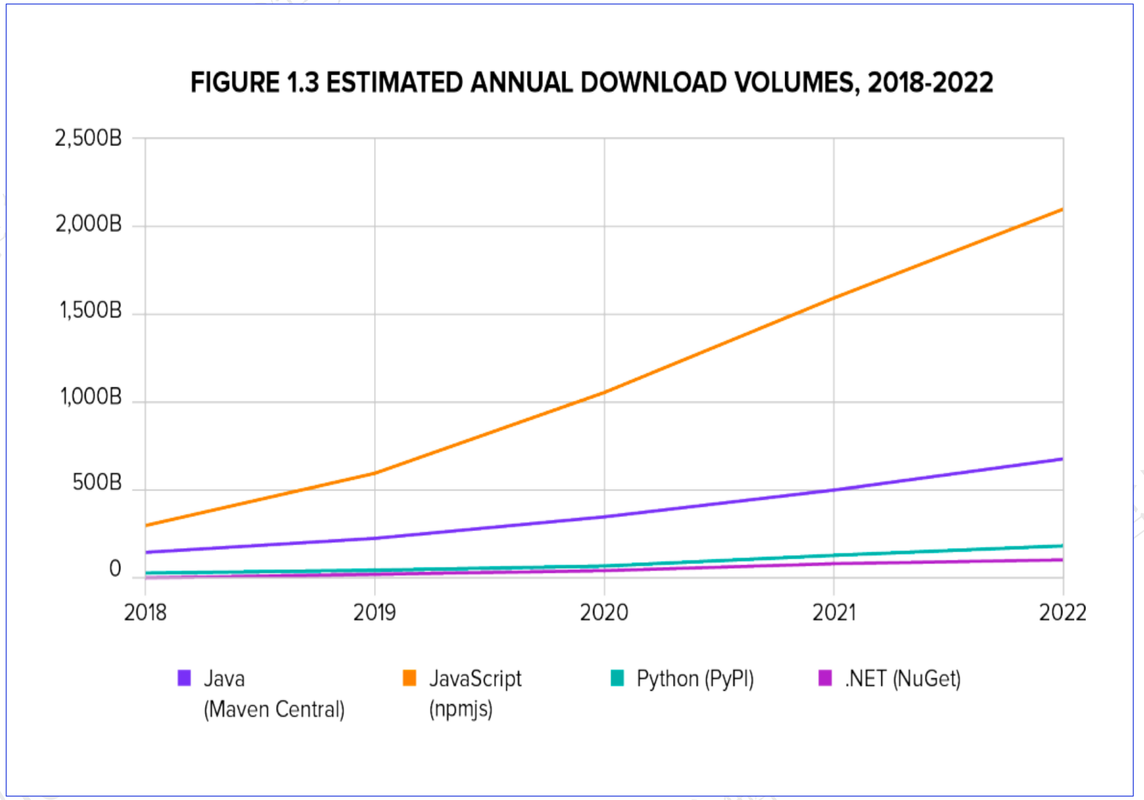
04 产品介绍

开源技术已成为企业信息化建设重要组成部分

墨菲安全 MURPHYSEC

国内 超九成 企业已经使用开源技术，开源技术已成为IT系统建设必不可少的部分

- Gartner ： 从 2010 年到 2018 年软件代码中采用开源框架或组件、第三方库的比例每年以 30%的速度增长
- Forrester：全球80%的软件包含开源组件
- Sonatype：预计2022年开源组件下载量超3万亿次
- 中国信通院：目前超过九成企业已经使用开源技术，开源技术已成为主流。
- 国内在 Gitee、Github等主流平台的贡献者数量 近5年均在不断攀升，我国现已排名全球第 二，人数接近千万。
- 2020年Gitee平台代码仓库增长率达157%， 开源项目数量达1500万。



开源技术的应用为企业带来三大严重安全威胁

墨菲安全 MURPHYSEC

65% 的代码项目存在许可证合规风险， 87% 的软件项目至少存在一个开源组件安全漏洞

开源组件

闭源商业

开源软件

私有源 → 代码开发 → 代码仓库

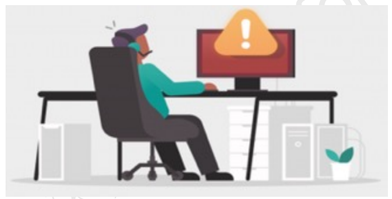
自研流程

部署运行 ← 制品及镜像 ← 编译构建

软件分发渠道

商采系统

办公环境



漏洞攻击

产权合规

供应中断

合规处罚

声誉损失

业务中断

数据泄露

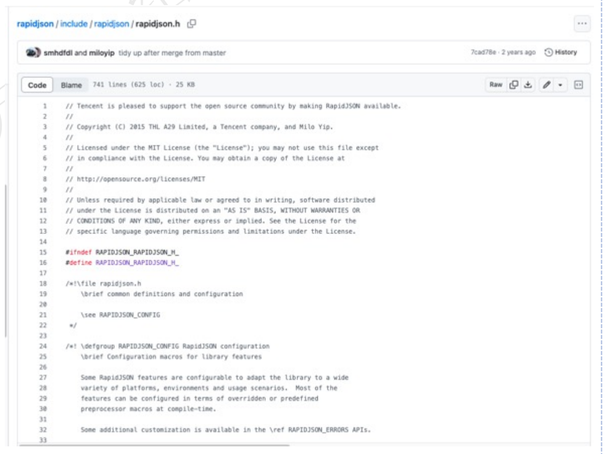
许可证风险引入

除通过开源组件/软件直接引入外，开源代码片段拷贝的方式也会导致开源许可证风险且更难发现

开源组件

开源软件

开源代码片段



开源许可证合规

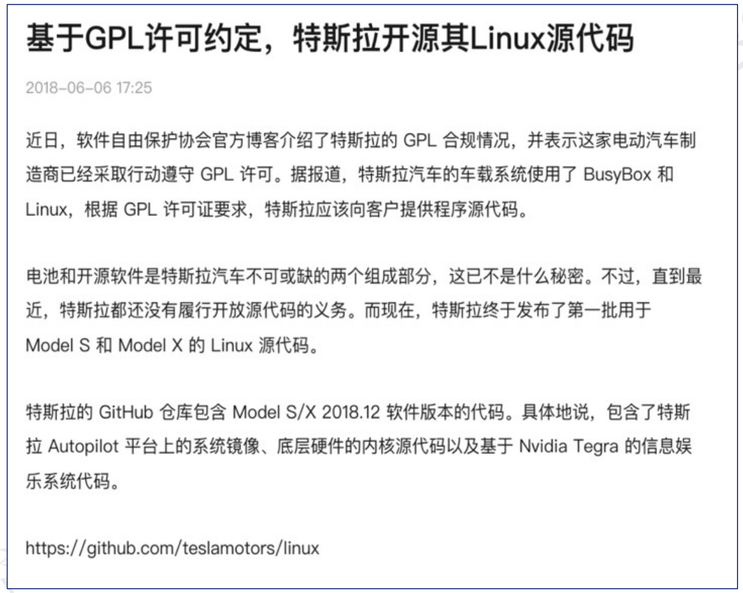
- **声誉损失**
- **法律处罚**
- **出海业务受阻**
- **软件著作权受损**

开源许可证合规风险事件

墨菲安全 MURPHYSEC

开源许可证合规风险导致企业声誉受损、经济损失、著作权受损

2018年，由于GPL许可证约束，特斯拉在软件自由保护协会（SFC）要求下开源Autopilot的linux内核和buildroot源码



基于GPL许可约定，特斯拉开源其Linux源代码

2018-06-06 17:25

近日，软件自由保护协会官方博客介绍了特斯拉的 GPL 合规情况，并表示这家电动汽车制造商已经采取行动遵守 GPL 许可。据报道，特斯拉汽车的车载系统使用了 BusyBox 和 Linux，根据 GPL 许可证要求，特斯拉应该向客户提供程序源代码。

电池和开源软件是特斯拉汽车不可或缺的两个组成部分，这已不是什么秘密。不过，直到最近，特斯拉都还没有履行开放源代码的义务。而现在，特斯拉终于发布了第一批用于 Model S 和 Model X 的 Linux 源代码。

特斯拉的 GitHub 仓库包含 Model S/X 2018.12 软件版本的代码。具体地说，包含了特斯拉 Autopilot 平台上的系统镜像、底层硬件的内核源代码以及基于 Nvidia Tegra 的信息娱乐系统代码。

https://github.com/teslamotors/linux

2021年12月，TikTok被曝出违法开源许可证协议，引发社区大量讨论和质疑，TT内部P0级事故

sina 财经头条 新浪财经APP

宏观经济 A股 港股 美股 基金 理财 黄金 期货 能源 互联网金融 房地产

套皮OBS？曝TikTok新品违反开源协议！

2021年12月21日 15:51 CSDN

整理 | 祝涛

出品 | CSDN（ID：CSDNnews）

近日，有推特用户称TikTok最新上线的软件TikTok Live Studio疑似使用了OBS (Open broadcasting Software)的源代码，但是却没有遵守相关的开源许可条款。OBS称已联系TikTok，但TikTok尚未对此事作出回应。

头条号入驻

CSDN 专业的中文 IT 技术社区

- Google开源offload友好协议PSP，目前已正署到生产中
- 如何将你的项目快速迁移到 GitCode?
- 27 岁的 Java，生日快乐！

2021年6月，国内首例由于违反GPL版权纠纷案裁判文书公示，标志着我国法律对开源许可证的认可

中国裁判文书网 China Judgements Online

济宁市罗盒网络科技有限公司诉被告福建风灵创景科技有限公司（以下简称福建风灵公司）、被告北京风灵创景科技有限公司（以下简称北京风灵公司）、被告深圳市腾讯计算机系统有限公司（以下简称腾讯公司）侵害计算机软件著作权纠纷一审民事判决书

案由 侵害计算机软件著作权纠纷 点击了解更多 案号 （2019）粤03民初3928号

发布日期 2021-06-30 浏览次数 1918

广东省深圳市中级人民法院

民事判决书

（2019）粤03民初3928号

墨菲安全

目录

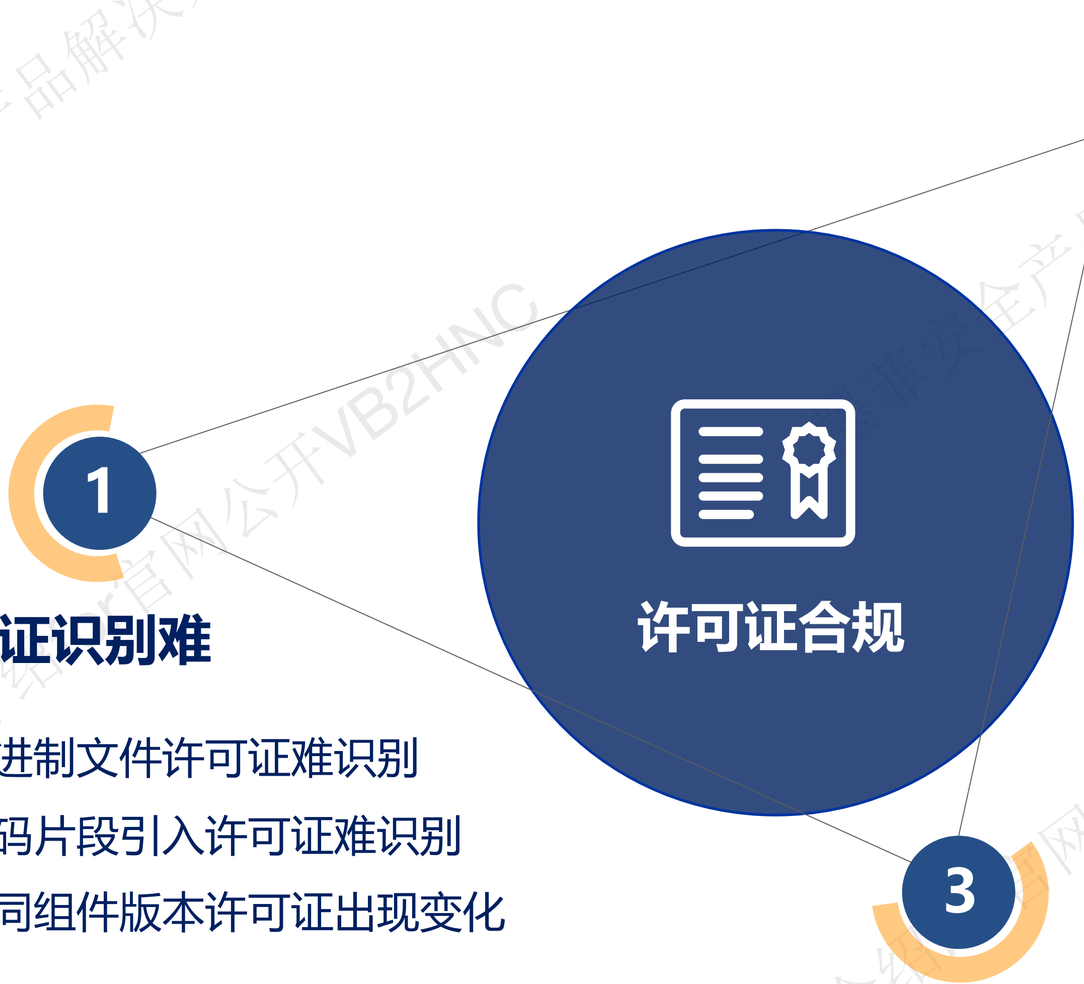
01 背景介绍

02 治理挑战

03 解决方案

04 产品介绍

开源许可证合规风险治理挑战



许可证识别难

- 二进制文件许可证难识别
- 代码片段引入许可证难识别
- 不同组件版本许可证出现变化

许可证风险评估难

- 许可证条款难解读
- 许可证风险场景不明确
- 不同许可证存在兼容性冲突

许可证风险整改难

- 许可证风险处置方式不明
- 替代组件评估选项成本高

墨菲安全

目录

01 背景介绍

02 治理挑战

03 解决方案

04 产品介绍

墨菲安全 开源许可证风险解决方案

墨菲安全 MURPHYSEC

行业领先工具+专家建设许可证风险识别、分析、卡位、处置闭环能力，助力企业控制开源合规风险

使用场景

- 软件出海知识产权合规
- 软件开源合规
- 车企出海知识产权合规

用户角色

- 法务
- 开源治理办公室
- 安全工程师
- 软件研发工程师

产品能力

开源组件准入管控

私有源安全网关

- 高危许可证拦截
- 基线设置
- 高风险组件审计
- Jfrog 接入配置
- nexus 接入配置

许可证风险检测

软件成分分析

- 许可证识别
- 许可证风险分析
- 许可证风险整改
- 专家验证
- 组件级许可证识别
- 文件级许可证识别
- 代码片段级许可证识别
- 源代码检测
- 二进制检测
- 固件检测
- APK 检测

核心技术

- 专业漏洞知识库
- 专业组件知识库
- 检测引擎

四大特性 解决开源许可证合规核心痛点

墨菲安全
MURPHYSEC

01 精准许可证识别

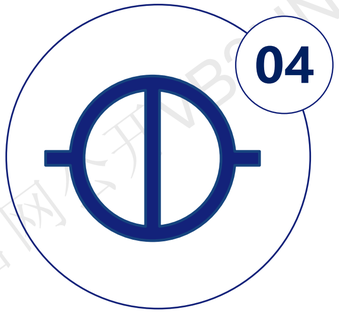
- 二进制/固件许可证识别
- 代码片段引入许可证识别
- 组件引入许可证识别

02 专业许可证信息

- 超3000类许可证数据
- 超2亿开源代码特征信息
- 详细的许可证风险场景解读

03 资深专家咨询

- 专家复核报告，保证过审
- 许可证场景解读
- 许可证风险整改指导



04 源头卡位

- 高风险许可证组件引入拦截
- 许可证风险处置成本降低80%

墨菲安全

目录

01 背景介绍

02 治理挑战

03 解决方案

04 产品介绍

产品一：软件成分分析（苏木）

墨菲安全 MURPHYSEC

SBOM分析

- 支持源代码及二进制
- 支持代码片段级分析
- 线上真实依赖识别，高准

风险检测

- 支持许可证识别
- 支持漏洞及投毒检测
- 漏洞线上真实影响分析
- 独家专业知识库

快速修复

- 许可证风险处置建议
- 组件升级兼容性评估

应用场景：产品交付阶段许可证风险处置

墨菲安全 MURPHYSEC

场景

企业出海或者项目开源场景下，必须接受严格的开源组件许可证合规审查

应用方案

预期效果

- ✓ 实时检测代码项目使用的开源组件及相关许可证风险
- ✓ 保障对外发布的代码项目许可证100%合规

产品二：源安全网关

墨菲安全
MURPHYSEC

网关插件

- 插件式一键安装
- 支持jfrog及nexus

JFrog

nexus repository

策略配置

- 黑白名单配置
- 支持观察模式及阻断模式
- 支持动态检测配置阻断

风险阻断

- 高风险许可证拦截使用
- 高危组件拦截下载

源安全网关-应用场景

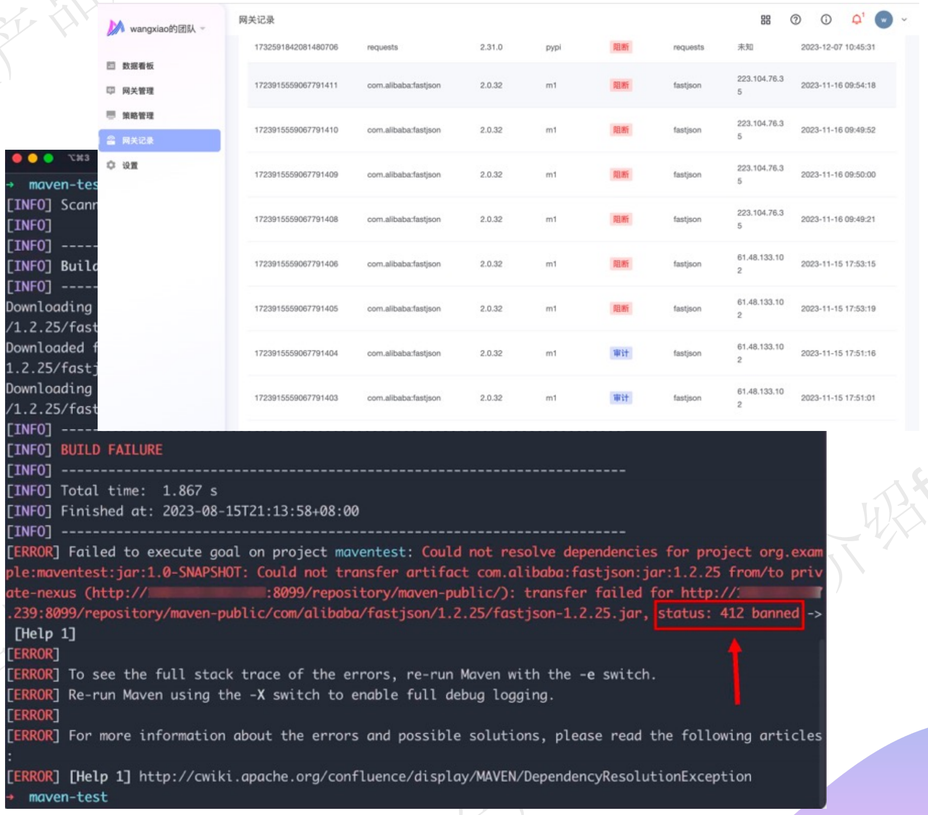
墨菲安全 MURPHYSEC

场景

经常出高危漏洞的及高风险许可证的组件需要严格准入准出管理

应用方案

发布组件管理制度 → 配置组件安全基线 → 先观察后拦截 → 查看系统拦截记录



预期效果

- ✓ 高风险许可证组件自动拦截
- ✓ 组件准入准出有序管理，先观察后拦截，可靠可控
- ✓ 突发0day漏洞&投毒事件，实时拦截应对，得心应手

产品对比

对比项	blackduck	墨菲安全	结论
安装&更新	私有化部署（知识库在云端，依赖海外网络）	私有化部署（知识库在云端，国内）	墨菲安全云端数据使用国内节点，网络延迟更低。
场景-license识别	支持	支持	基本持平
场景-license兼容性	未知	无	blackduck能力未知
场景-逐行对比	以N行代码为单位匹配	通过语义分析以函数为单位匹配	blackduck召回率较高，墨菲准确率较高
场景-copyright扫描	提示使用license类型	提示使用license类型及风险场景	墨菲提示license类型的同时提示风险场景，运营成本更低
更新速度	天级	小时级	更新简单可控，可随时下载最新知识库上传至服务更新。
行业选择	蔚来、字节	快手、平安	blackduck产品推广更早，占有率更高，墨菲安全作为新企业，发展快
KB库	2000+开源协议	3000+开源协议	墨菲安全在开源协议收集上更具优势、常见组件特征丰富，blackduck在其他组件样本特征上更具优势
	57亿+组件特征库	40亿+组件特征库	

某地图服务商G实施案例

墨菲安全
MURPHYSEC

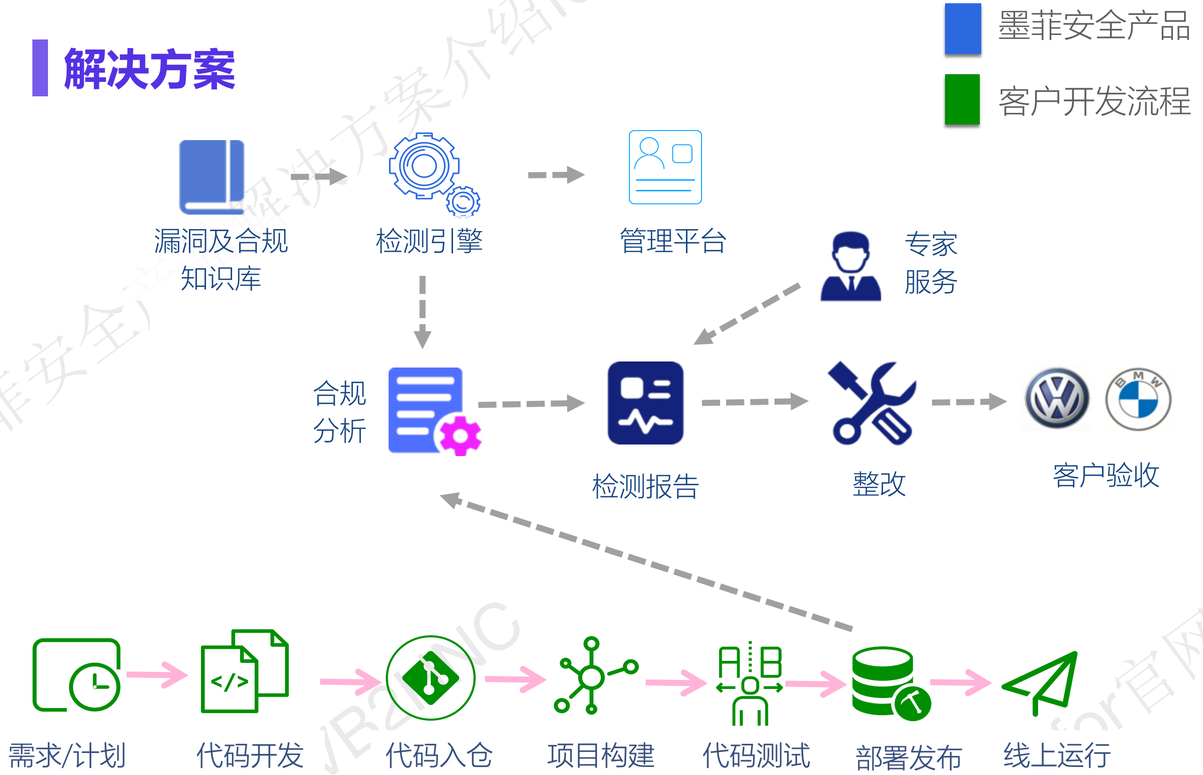
客户痛点

① 客户的SDK/APK服务于大众、宝马等大量国内外知名车企，客户需严格审查代码许可证合规
② 车企客户对于交付的所有安装包需要严格审查是否存在严重安全漏洞

挑战

① 人工审查效率低、工具的能力参差不齐，客户用了多款不同的工具
② 覆盖率无法保障，误报及漏报都很高
③ 发现安全问题及许可证合规的组件后不知如何修复

解决方案



收益

① 使用墨菲安全平台识别准确率提升50%
② 墨菲安全专家提供发布前的专家确认，保障100%交付无问题
③ 一些很难修复的问题墨菲安全专家提供100%保障

公司发展历程

墨菲安全 MURPHYSEC

2020.05

来自百度、华为为主的核心团队组建，启动墨菲安全漏洞知识库建设

2021.09

产品v1.0正式版本发布，适配主流DevOps流程及工具

2021.11

完成顶级投资机构红杉资本数千万天使轮融资

2022.03

产品2.0发布，接入平安、快手等第一批头部客户

2022.12

墨菲安全签约十数家互联网、金融、运营商客户

2023.05

墨菲安全软件供应链安全v3版本发布，全球首发可达性风险及兼容性评估技术

2023.12

墨菲安全入选国家高新技术企业，签约数十家互联网、金融、运营商客户

联系我们

墨菲安全
MURPHYSEC

公司地址：

北京市海淀区百旺弘祥(弘祥1989)文创园

联系人：

杨女士

联系电话：

400 180 9568

官网：

https://www.murphysec.com/