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

开源组件安全风险治理方案

2024.01

关于墨菲安全

懂客户 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；

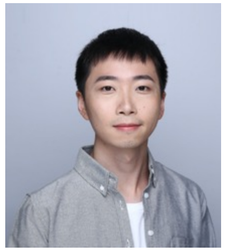
产品技术领先 顶级的漏洞研究及应用安全实践经验，创始人曾在乌云主导国内首款检测SaaS产品TangScan；

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

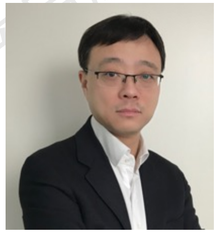


联创&实验室负责人 欧阳强斌

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 · CSCEC · 中国建筑 CHINA STATE CONSTRUCTION · 理想

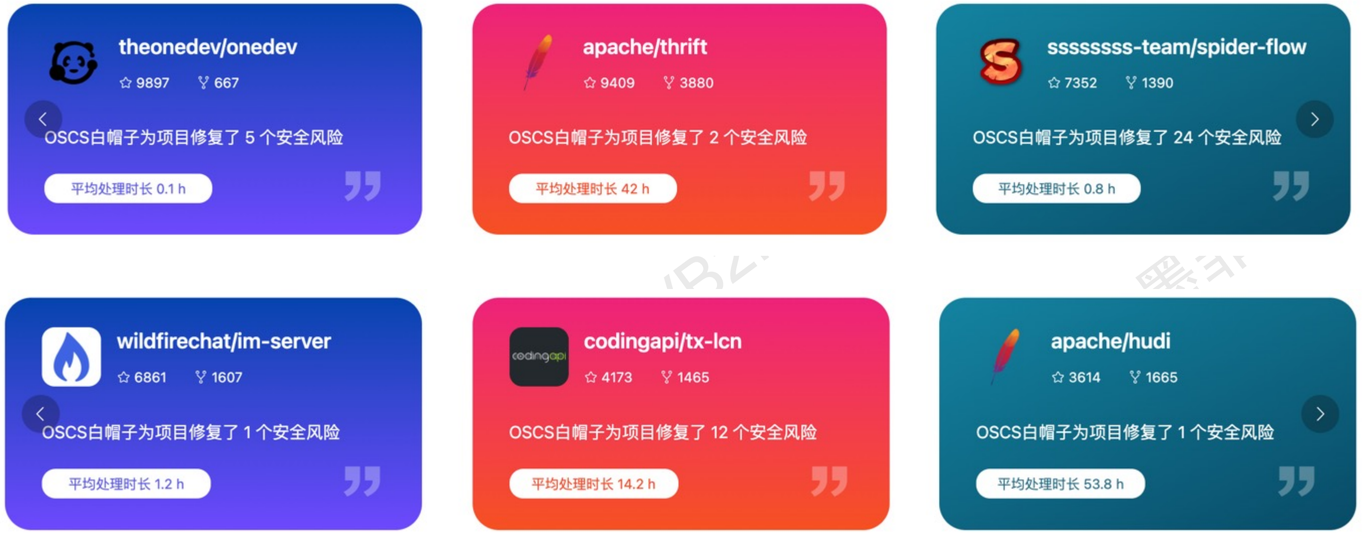
监管合作

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

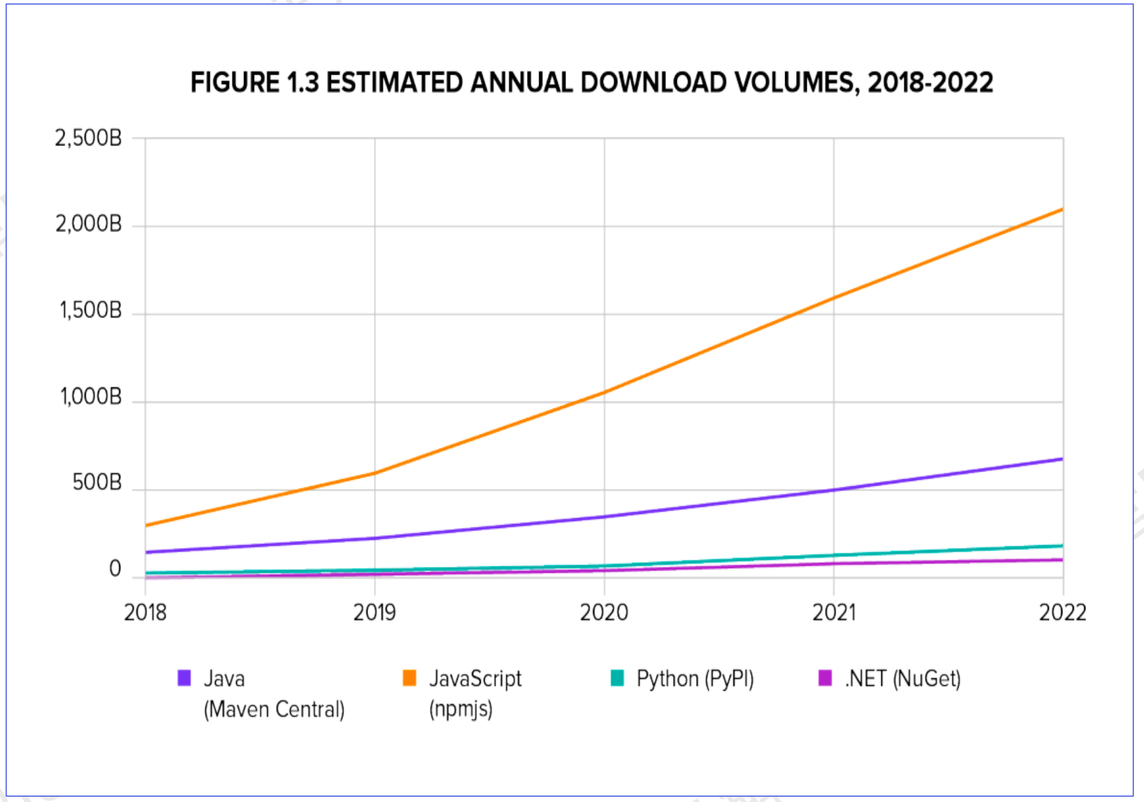
专业、专注、可靠

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

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

开源组件 LOG4J Spring MVC

闭源商业 ORACLE cisco

开源软件 hadoop NGINX

私有源 JFrog nexus repository → 代码开发 IJ → 代码仓库 SVN

自研流程

部署运行 ← 制品及镜像 Harbor JFrog ← 编译构建

软件分发渠道 亚马逊 aws android GitHub Apache Maven tuna 清华大学开源软件镜像站

商采系统 ERP OA

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

开源风险事件频发，已成为企业面临的严重安全威胁

墨菲安全 MURPHYSEC

漏洞攻击

2021年12月，Log4j2曝出严重漏洞，可直接获取服务器权限，影响范围极广，大量企业抱怨修复困难

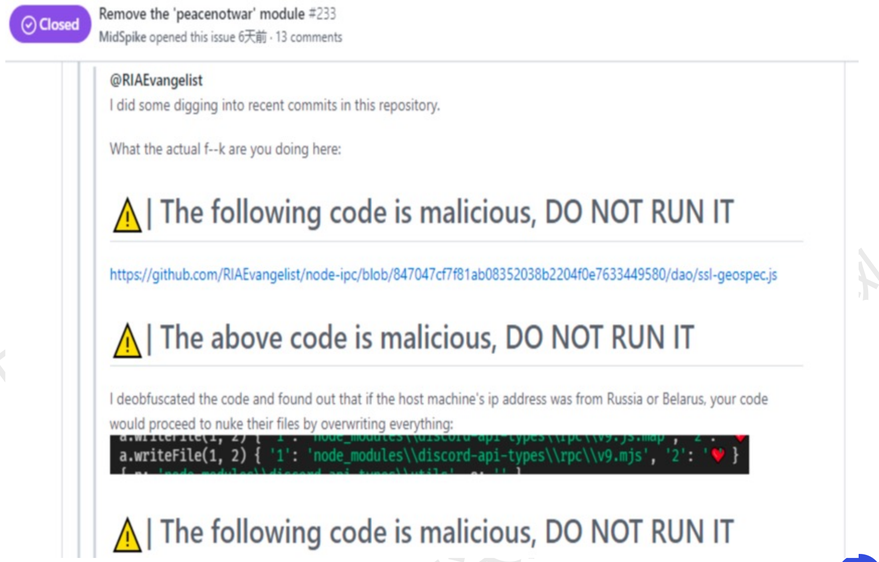
Qualys威胁研究小组(TRU)发布的最新报告显示2023年共披露了**26447**个漏洞，比上一年增加了**1500**多个CVE， 97个可能被利用的高风险漏洞不在CISA已知被利用漏洞目录中，**25%的高风险漏洞**在发布当天就被利用

产权合规

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

供应中断

2022年03月，以反战为名，node-ipc包作者进行供应链投毒，破坏系统文件，修改用户的所有文件为❤️



Sonatyoe第九届软件供应链安全报告指出，截止2023年9月年内共发现**245032**恶意软件包为2022年的**3倍**，恶意软件包已成为下一代软件供应链攻击主要方式之一。

国家高度重视软件供应链安全，相关监管政策密集出台

墨菲安全 MURPHYSEC

2020

- 《关于开展金融科技应用风险专项摸排工作的通知》

2021

- 《金融网络安全 Web应用服务安全测试通用规范》
- 《关键信息基础设施安全保护条例》
- 《网络产品安全漏洞管理规定》
- 《关于规范金融业开源技术应用与发展的意见》

2022

- 《信息安全技术软件供应链安全要求》国标征求意见稿
- 《金融科技发展规划（2022-2025 年）》
- 《医疗器械网络安全注册审查指导原则2022年修订版》

2023

- 《证券公司网络和信息安全三年提 升计划（2023-2025 年）》
- 《汽车整车信息安全技术要求（征求意见稿）》

中国人民银行办公厅 中央网络安全和信息化委员会办公室秘书局 工业和信息化部办公厅 中国银行保险监督管理委员会办公厅 中国证券监督管理委员会办公厅关于规范金融业开源技术应用与发展的意见

标题： 中国人民银行办公厅 中央网络安全和信息化委员会办公室秘书局 工业和信息化部办公厅 中国银行保险监督管理委员会办公厅 中国证券监督管理委员会办公厅关于规范金融业开源技术应用与发展的意见

索引号： HB/2021-4364505　　**文号：** 银办发〔2021〕146号

发文机关： 中国人民银行办公厅 中央网络安全和信息化委员会办公室秘书局 工业和信息化部办公厅 中国银行保险监督管理委员会办公厅 中国证券监督管理委员会办公厅　　**公文种类：**

发布日期： 2021年10月20日

生效日期：

主题词： 金融业开源技术

22/23年国家大型攻防演练中，软件供应链安全的攻击重点加分

供应链安全得分点

攻击队从防守方供应链（的系统）获取到参演单位的重要数据(个人信息、生产数据、重要文件、源代码、敏感系统管理信息等)，**可获得 200-500 分不等的加分。**

目录

墨菲安全
MURPHYSEC

专业、专注、可靠

开源风险治理的四大挑战

墨菲安全 MURPHYSEC

开源组件管控难

① 开源组件版本安全性难评估

② 缺乏有效的准入控制手段

③ 开源组件依赖数量巨大

④ 安全性与业务需求冲突

资产依赖庞杂

① 直接及间接依赖链路复杂

② 二进制文件SBOM识别难

③ 多语言组件依赖特性差异

④ 代码片段依赖难识别

⑤ 线上服务器依赖识别难

漏洞修复困难

① 单个项目漏洞数量太多

② 修复升级兼容性问题多

③ 老项目开源组件无法升级

④ 研发排斥/不认可风险

应急响应难

① 每天数百起0day漏洞

② 缺乏及时有效的漏洞情报

③ 突发风险无法快速定位

④ 突发风险不知如何处置

目录

资产台账为抓手，打造软件供应链安全治理框架

墨菲安全 MURPHYSEC

管理体系

制度　流程　规范

控制体系

软件供应链主要管控对象

开源组件　开源软件　闭源软件

三大风险

漏洞攻击　中断供应　产权合规

事前 准入预防

开源选型　资产台账　安全基线

准入准出　私有源拦截　商采准入

事中 持续管理

成分分析　二进制检测　漏洞检测　镜像扫描

许可证识别　漏洞修复　代码溯源　自查整改

事后 应急处置

漏洞情报　投毒情报

应急止损　威胁溯源

产品能力

准入评估　准出卡位

私有源管理　引入提醒

源安全网关

SBOM清单　风险检测

许可证检测　快速修复

软件成分分析

0day漏洞情报　资产录入

投毒漏洞情报　漏洞处置

漏洞&投毒情报

软件供应链资产台账

软件供应链风险管理平台

核心技术

专业漏洞知识库　专业组件知识库　检测引擎

墨菲安全

面向开发者打造 企业级软件供应链安全云平台

墨菲安全 MURPHYSEC

用户

研发工程师 | 安全工程师 | DevOps工程师 | 运维工程师 | 法务 | 工程管理人员

软件供应链安全云平台

用户功能

- 商采软件审查
- 开源漏洞检测
- 漏洞快速修复
- 许可证分析
- 供应链资产台账
- 应急指南
- 0day/投毒预警
- 风险组件拦截
- 开源组件选型推荐
- 组件安全基线
- 云平台门户
- 漏洞真实影响分析
- 代码安全漏洞

产品能力

- 软件成分分析
- 资产及漏洞情报
- 源安全防火墙
- 静态代码扫描

核心技术

- 专业漏洞知识库
- 专业代码特征库
- 专业代码分析引擎
- AIGC

关联能力

- 账号体系
- CMDB
- HIDS
- DevSecOps
- DevOps

自研软件开发流程

私有源 → 代码开发 → 编译构建 → 制品仓库 → 上线部署

商采软件

测试 → 采购 → 部署

办公软件

下载 → 安装

四大特性 直击开源治理核心痛点

墨菲安全
MURPHYSEC

01

行业领先知识库(SRKB)

- 百度/乌云十年经验积累
- 每条漏洞数据承诺核准
- 25+独家漏洞字段，助力深度检测
- 80+/周的独家0day&组件投毒覆盖

02

漏洞快速修复闭环

- 领先的漏洞可达性分析技术
- 超十亿的组件升级兼容性评估
- IDE/Gitlab一键修复91%成功率

03

高质量情报预警

- 漏洞&投毒情报93%快于同行
- 漏洞影响资产自动排查
- 漏洞处置方案清晰明确
- 应急响应效率提升80%

04

源头风险卡位

- 安全左移至私有源头
- 配合企业开源组件准入准出管理
- 投毒组件自动拦截
- 风险处置成本降低80%

目录

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

- 支持漏洞及投毒检测
- 支持许可证识别
- 漏洞真实影响分析
- 独家专业漏洞知识库

快速修复

- 组件升级兼容性评估
- 编码阶段漏洞一键修复
- 支持多种处置方案
- 组件负责人自动关联

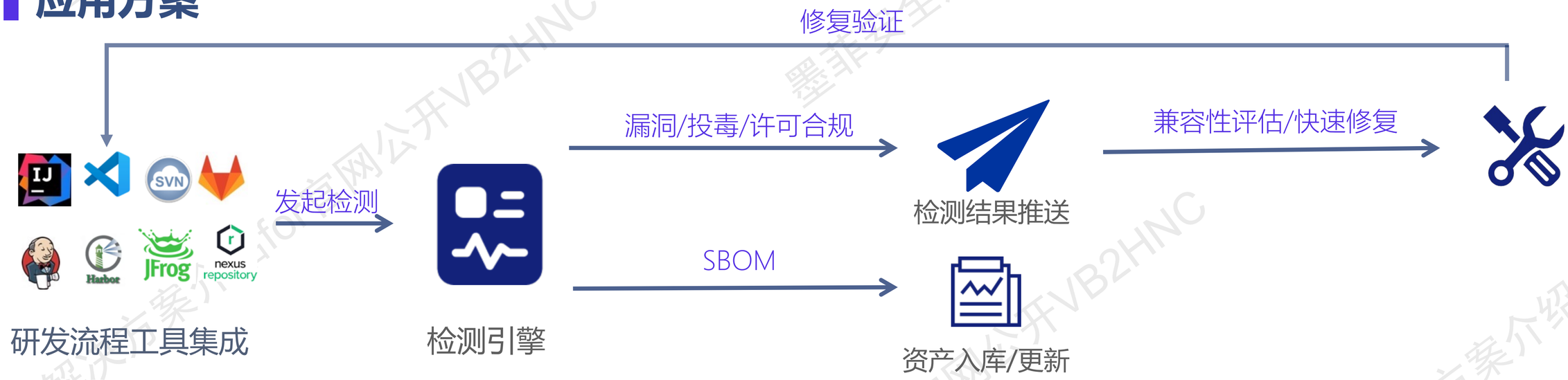
应用场景：研发过程中资产及风险管理

墨菲安全 MURPHYSEC

场景及痛点

自研软件大量依赖开源组件，其中开源漏洞频发，项目开源资产及风险不明，漏洞修复兼容性难评估

应用方案



预期效果

- ✓ 开源资产及风险及时发现，保障线上发布代码安全提升90%
- ✓ 项目组件漏洞一目了然，风险可量化管理，安全运营成本降低80%

应用场景：商采软件准入及风险管理

墨菲安全 MURPHYSEC

场景及痛点

商业外采软件一般以制品形式交付，其中包含的开源资产及风险不可知，存在的开源风险可能被利用导致企业数据被窃取/数据加密勒索；

典型客户

中国移动 China Mobile

兴业证券 INDUSTRIAL SECURITIES

应用方案

预期效果

- ✓ 所有外采商业软件需经过安全测评，风险可见，促使厂商提升安全
- ✓ 外采商业软件依赖的三方资产录入资产台账统一管理，方便后续应急处置

多种检测模式灵活适配多应用场景

墨菲安全 MURPHYSEC

模式	检测内容	适用场景	检测效率/速度
标准模式	1.智能识别检测对象中包含的各语言源代码、二进制文件，进行深度检测 2.支持真实影响分析、是否编译扫描的配置开关	1.对一个复杂项目进行 周期性的全面扫描 2.对扫描效率要求不是特别高的场景	一般 ~ 快 （跟文件大小有关）
依赖配置扫描	1.智能识别检测对象中包含的各语言源代码 2.支持真实影响分析、是否编译扫描的配置开关	1.将墨菲安全检测 集成至CI/CD流水线，实现安全门禁	快 ~ 极快 （跟私有源速度相关）
容器镜像扫描	1.对容器镜像中依赖的中间件程序进行安全风险监测 2.对容器镜像中应用程序源码/二进制进行检测	1.单个容器镜像检测 2.与harbor等容器镜像仓库集成检测	一般 ~ 快 （跟文件大小有关）
二进制扫描	1.对各语言编译的二进制文件进行软件成分分析及安全风险检测	1.对软件供应商/外包团队交付的制品文件进行风险检测和确认 2.对自己研发的软件对外发布之前的制品进行风险检测和自查	快 ~ 极快 （跟文件大小有关）
固件扫描	1.对不同CPU架构及不同开发语言的固件进行软件成分发分析及安全检测	1. .对自己研发的软件对外发布之前的固件制品进行风险检测和自查 2. 对外部采购的软件的固件进行二次检测确认	快 ~ 极快 （跟文件大小有关）

产品二：资产管理及漏洞情报（贯众）

墨菲安全 MURPHYSEC

资产台账

- SBOM导入
- 系统及三方资产导入
- 负责人标签
- 资产风险等级标签
- 资产指纹识别

情报预警

- 公开0day分析及预警
- 独家0day漏洞分析预警
- 组件投毒情报分析及预警

应急处置

- 自动关联受影响资产
- 自动化预警配置
- 临时缓解处置方案
- 专业的漏洞应急指南

资产及漏洞情报—应用场景

墨菲安全 MURPHYSEC

场景

爆出突发漏洞，企业需及时排查是否受影响，并快速处置

应用方案

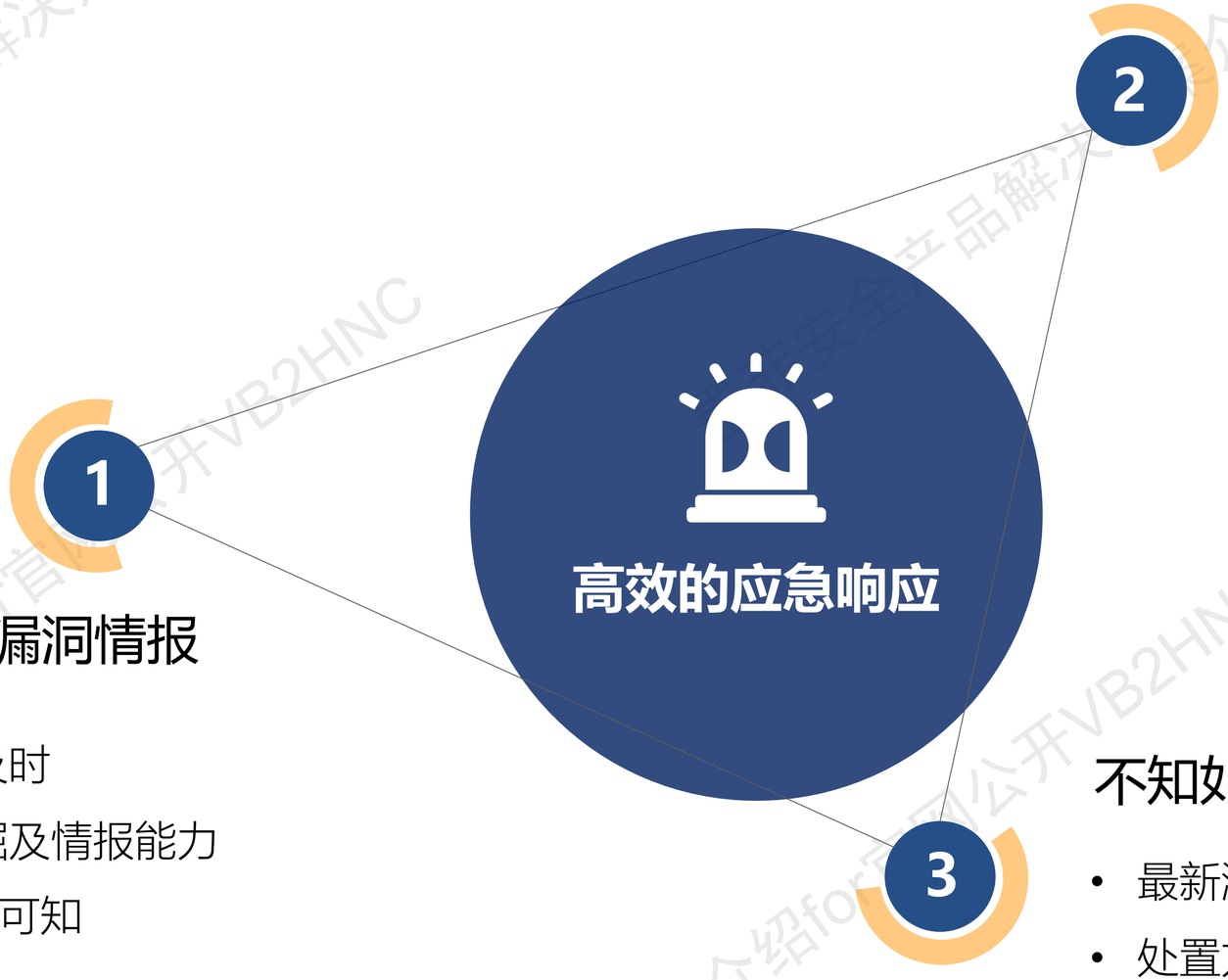
预期效果

✓ 第一时间拿到情报并自动关联出受影响的资产，快速完成止损和修复

✓ 老板问起来时已经处理完了！

企业0day漏洞及投毒应急的痛点

墨菲安全 MURPHYSEC



缺乏及时有效的漏洞情报

- 最新漏洞获取不及时
- 缺乏最新投毒挖掘及情报能力
- 漏洞真实&影响不可知

不知哪些资产是否受影响

- 企业软件供应链资产覆盖不全
- 资产归属不清晰
- 资产列表的持续更新难度大
- 资产和最新漏洞关联不起来

不知如何快速处置止损

- 最新漏洞的临时处置方案不清晰
- 处置方案的副作用难评估

产品三：源安全网关（京墨）

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

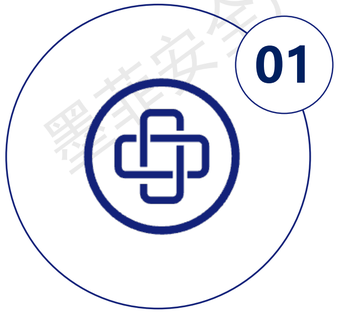
- 组件安全基线配置
- 黑白名单配置
- 支持观察模式及阻断模式
- 支持动态检测配置阻断

风险阻断

- 高危组件拦截下载
- 高风险许可证拦截使用
- 高危0day漏洞拦截止损
- 投毒组件屏蔽隔离

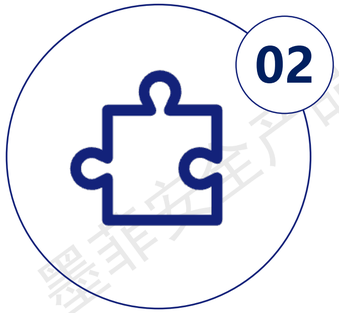
四大高危风险场景覆盖

墨菲安全
MURPHYSEC



01 高危开源组件准入准出

- Fatjson/Log4j2等高危组件拦截
- 配合企业开源管理制度落地管控



02 企业内部二方组件管控

- 企业内部公共组件风险拦截
- 避免内部二方组件风险扩散

03 投毒组件自动化拦截

- 自动拦截全网投毒风险组件
- 覆盖npm/pip/ruby/java等

04 高危许可证组件准入准出

- 类GPL高危许可证组件实时拦截
- 自定义许可证级别和拦截策略

源安全网关-应用场景

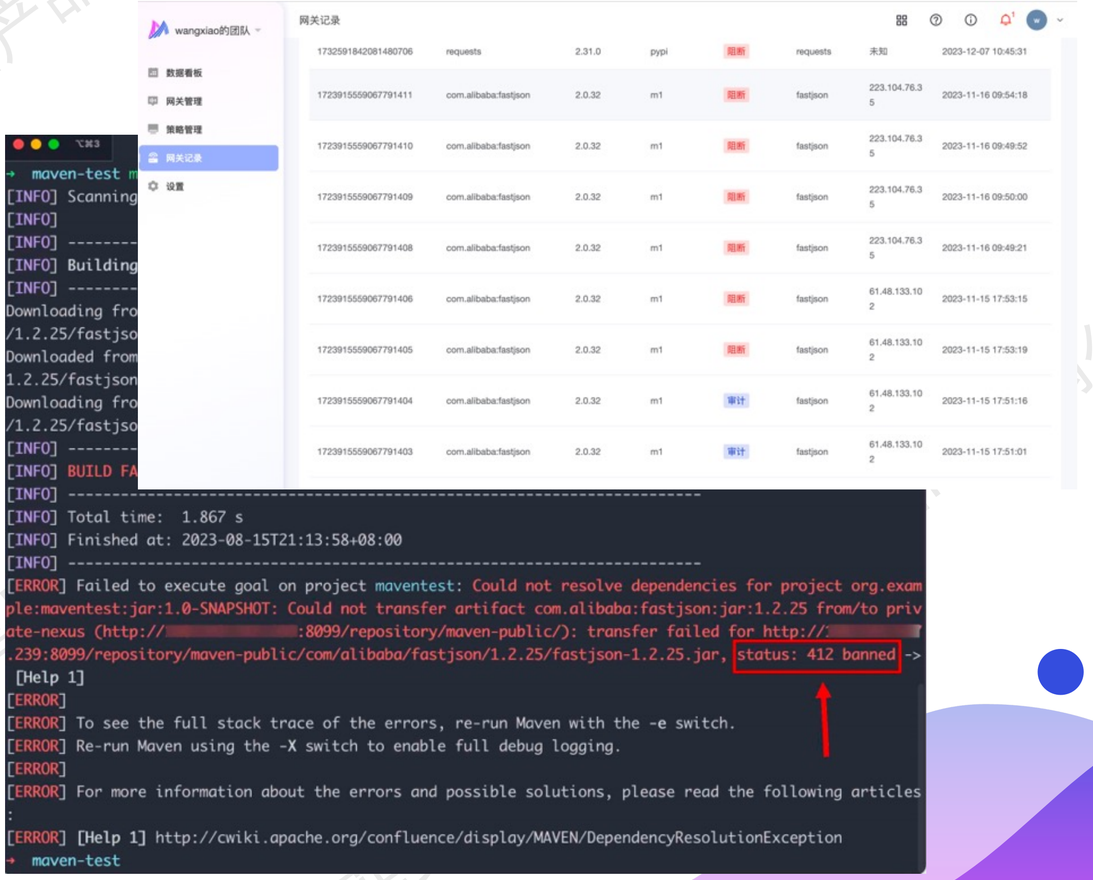
墨菲安全 MURPHYSEC

场景

配合开源管理制度，对四大风险场景的开源组件实施严格准入准出管理

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

- ✓ 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

某证券客户X实施案例

墨菲安全
MURPHYSEC

客户痛点

① **证券自研及外采系统都普遍采用了大量开源组件；
② 这些开源组件存在大量安全漏洞；
③ 给**证券的数据安全及合规带来巨大挑战；

挑战

① 复杂度高：开源组件分布分散，且版本众多，统计识别难度都很大
② 依赖性强：很多系统都直接间接依赖大量开源组件，出现安全漏洞后也不敢轻易升级，容易导致兼容性问题
③ 冲突性大：研发与安全部门的目标不一致；开源软件在不同系统版本不一致；开源软件安全评估和准入流程不一致；这三个不一致导致各方合作起来冲突较大

解决方案

① 建立开源软件安全管理机制和流程，并在各阶段持续性进行安全评估
② 引入墨菲安全的软件供应链安全平台（SCA+源安全网关）支撑治理体系落地

#客户对外分享治理思路

收益

① 外采软件实现全流程的开源软件安全风险治理，将安全风险卡在上线前
② 自研软件中的开源软件实现全流程管控，有效降低安全风险

某互联网客户K实施案例

墨菲安全
MURPHYSEC

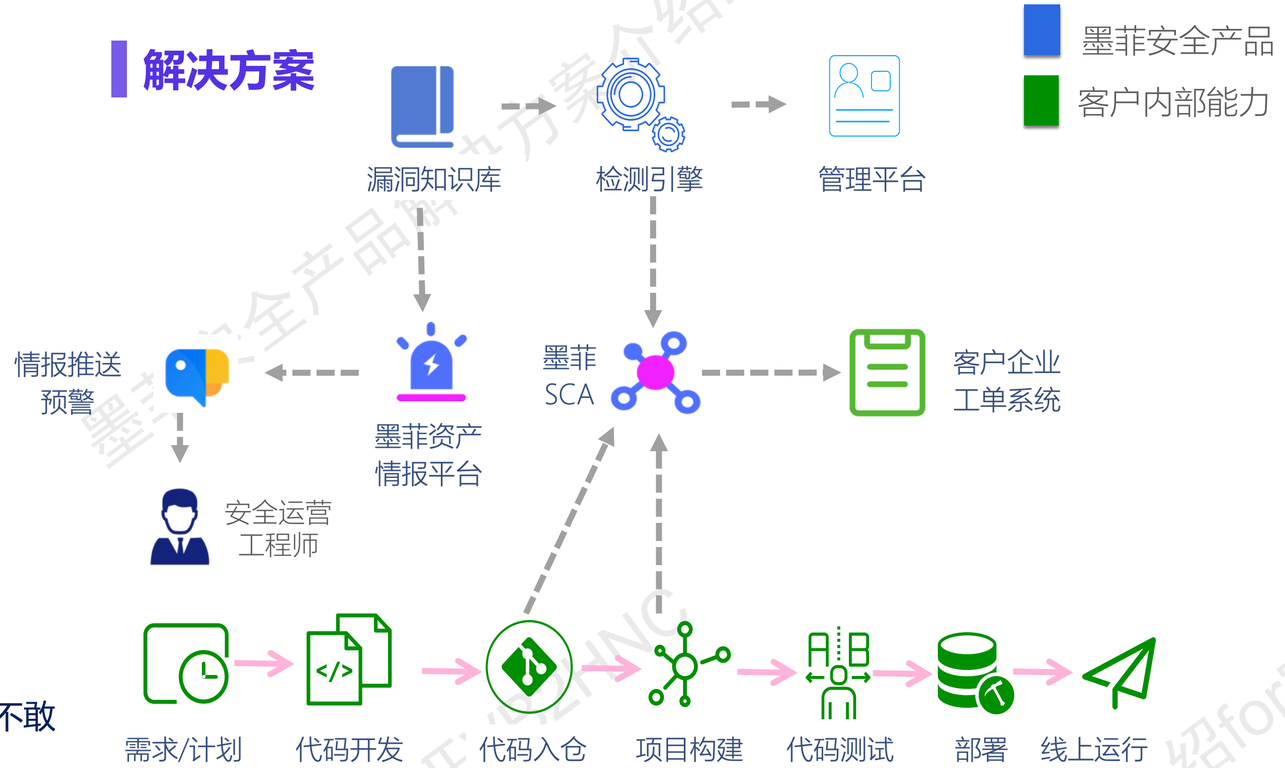
客户痛点

① SRC每年收到的漏洞大量都来自开源组件的通用0day
② 遇到类似log4j2这样的0day，无法快速排查响应
③ 公司存在出海业务，需要排查代码中是否存在许可证合规风险

挑战

① 复杂度高：开源组件分布分散，且版本众多，统计识别难度都很大
② 依赖性强：很多系统都直接间接依赖大量开源组件，出现安全漏洞后也不敢轻易升级，容易导致兼容性问题
③ 业务强势：业务部门的研发很强势，也很懂技术，对安全发的工单质疑必要性和专业性，需要安全给出演示

解决方案



收益

① 自研流程实现开源组件安全漏洞的实时检测/上线前卡位，高危漏洞下降90%
② 0day漏洞从获取情报到应急处置，全过程效率从天级下降到小时级

某保险客户D实施案例

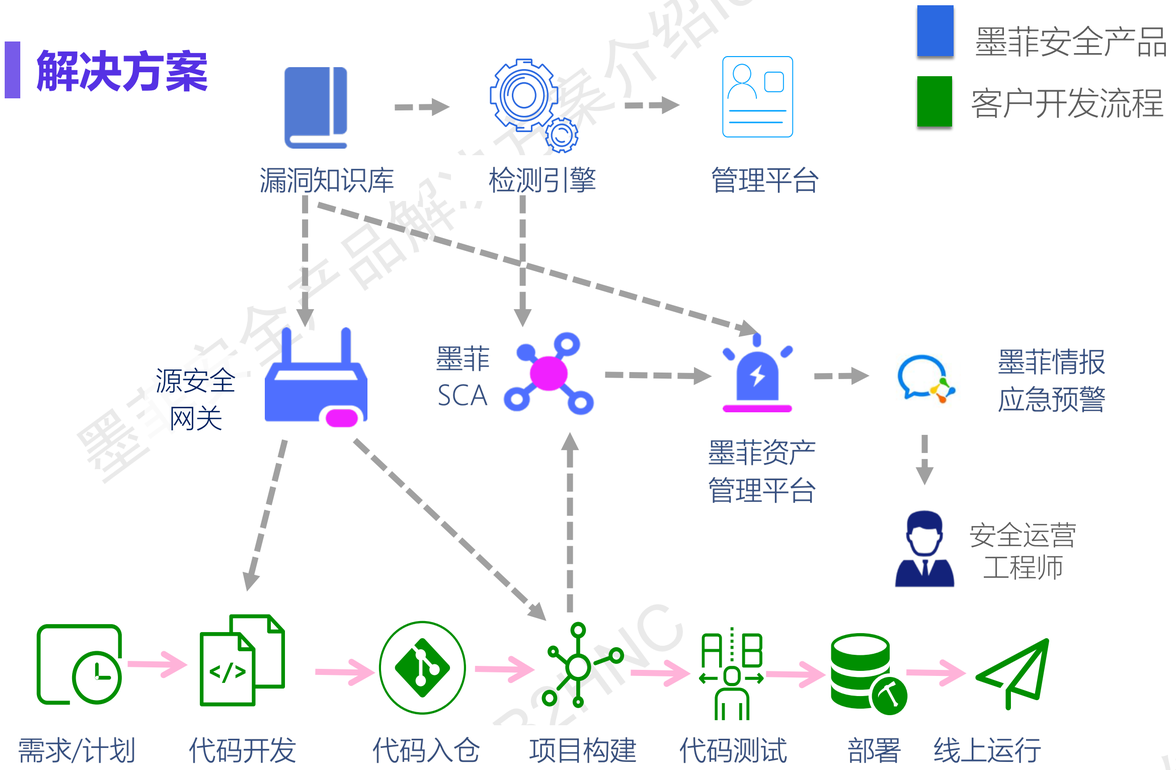
客户痛点

1）不知道线上到底有多少有缺陷的组件和漏洞
2）漏洞修复修复成本高
3）突发漏洞响应及时度不够，处置成本高
4）组件引入难管控

挑战

✓ 内部系统较多，资产识别难度也大
✓ 漏洞修复兼容性难以评估
✓ 每天外部曝出的漏洞太多，跟不过来
✓ 每次系统更新都有大量新组件引入，新引入组件风险不明

解决方案



收益

✓ 安全能能力嵌入研发流程，新增风险及时感知
✓ 线上组件漏洞一目了然，风险可量化管理
✓ 高风险组件自动拦截，降低业务安全风险
✓ 突发漏洞及时感知，应急处置效率提升80%

产品对比

墨菲安全 MURPHYSEC

产品	对比项		墨菲安全	某海外成熟产品	某国内成熟产品
苏木-软件成分分析	检测支持	源码检测语言支持	支持语言包括：C/C++、Golang、Java、PHP、Python等18种语言	支持语言包括：C/C++、Golang、Java、PHP、Python等18种语言	Java、Python、JavaScript、php、Go\Golang、Scala、等15种语言（不包含C/C++）
		二进制制品分析	支持制品、压缩包、安装包、原生二进制、固件等多种形态	支持制品、压缩包、安装包、原生二进制、固件等多种形态	仅支持jar、war、rar、tar4种制品格式
		混合形态检测支持	支持不同语言源码、不同形态制品混合递归分析检测	支持混合检测	不支持源码与二进制混合检测
	漏洞数据	漏洞知识库数量	覆盖国内外权威漏洞库、在野漏洞、墨菲私有漏洞，漏洞数据41W+	漏洞总量20万+,CVE漏洞库及3000+CVE未收录漏洞	涵盖NVD、CNVD、CNNVD、开源社区漏洞信息，漏洞数据18W+
		许可证数量	覆盖目前识别到的3000+许可证	2750+	500个
		漏洞信息丰富程度	除官方漏洞基础信息之外，还包含漏洞缺陷点、是否有POC&EXP、以及利用条件等漏洞深度信息	官方漏洞数据基础信息	只包含官方漏洞数据基础信息
	检测内容	开源组件漏洞检测	支持	支持	支持
		开源组件许可证风险检测	支持	支持	支持
		缺陷组件真实调用分析	支持java、JavaScript	支持java	不支持
		代码溯源分析	支持	支持	不支持
	漏洞修复	漏洞修复优先级	支持	支持，提供自有漏洞影响评级	不支持
		gitlab一键PR	支持	不支持	不支持
		IDE一键修复	支持	不支持	不支持
		升级版本的兼容性评估	支持	不支持	不支持
京墨-源安全网关	源安全网关	源头风险卡位	支持	不支持	不支持
贯众-资产及漏洞情报	风险情报预警	漏洞情报预警	支持	不支持	不支持
		投毒情报预警	支持	不支持	不支持

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

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/