墨菲安全
MURPHYSEC

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

汽车软件供应链安全及合规解决方案

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；

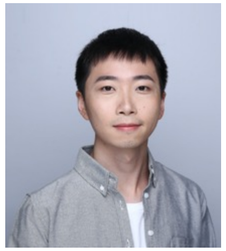
产品技术领先 顶级的漏洞研究及应用安全实践经验，创始人曾在乌云主导国内首款检测SaaS产品TangScan；

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

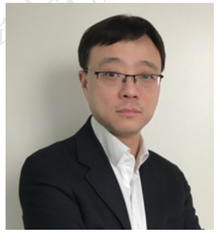


联创&实验室负责人 欧阳强斌

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

运营商及能源

中国移动 China Mobile　天翼云　国家电网 STATE GRID

车及供应链

理想　AUTEL 道通　高德地图

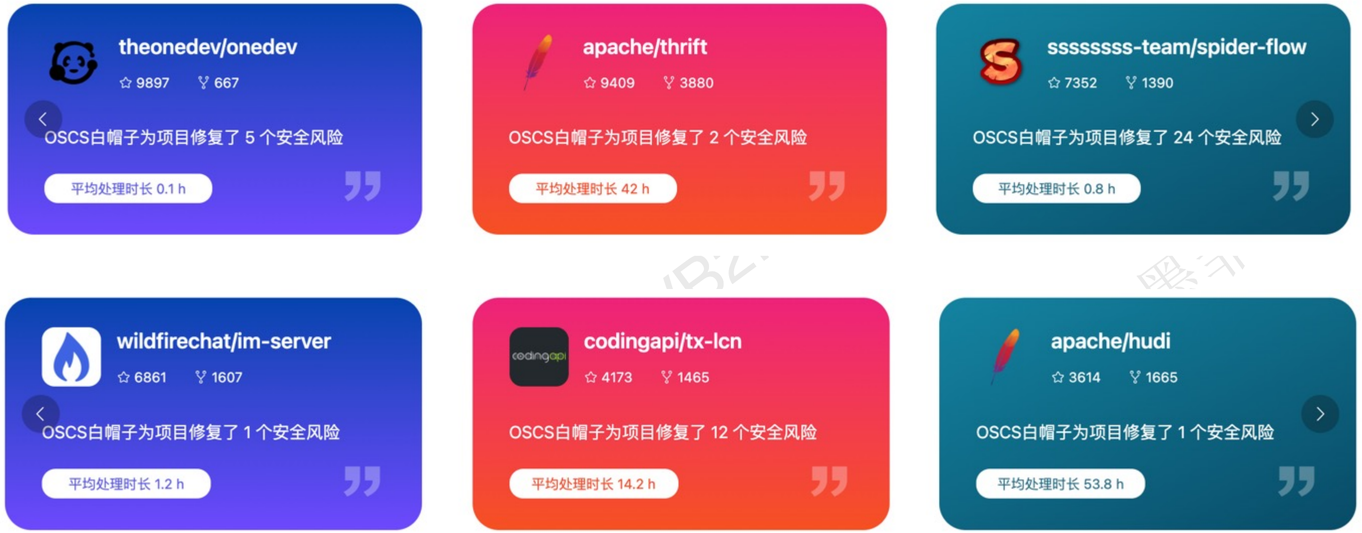
监管合作

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

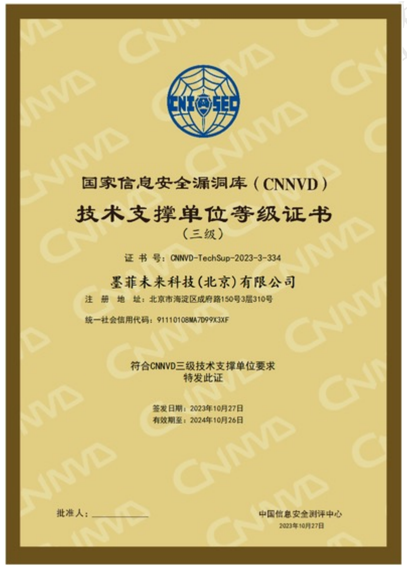
750万 累计发现漏洞数

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

墨菲安全

目录

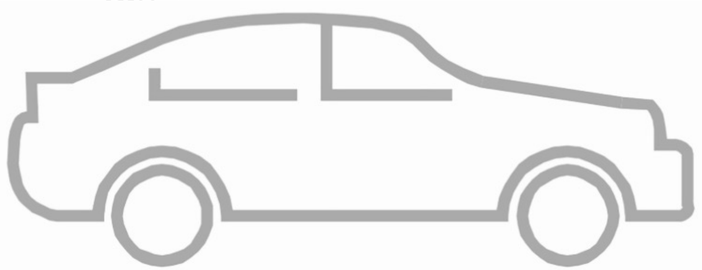
墨菲安全
MURPHYSEC

专业、专注、可靠

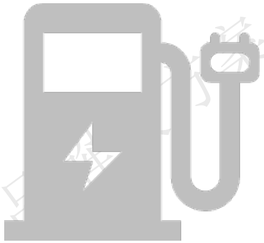
软件定义汽车下的复杂产品

墨菲安全 MURPHYSEC

41%的攻击来自云端



100个ECU和1亿行代码



配套基础设施

移动端

合规要求高 → 车辆安全涉及人身安全，数据安全、漏洞管理要求高

风险暴露面广 → 云、车、端资产众多，风险暴露面广，安全防护难度大

供应链复杂 → 80%硬件&固件来自200+上下游供应商

Tier1

BOSCH DENSO 德赛西威 HARMAN

Tier2

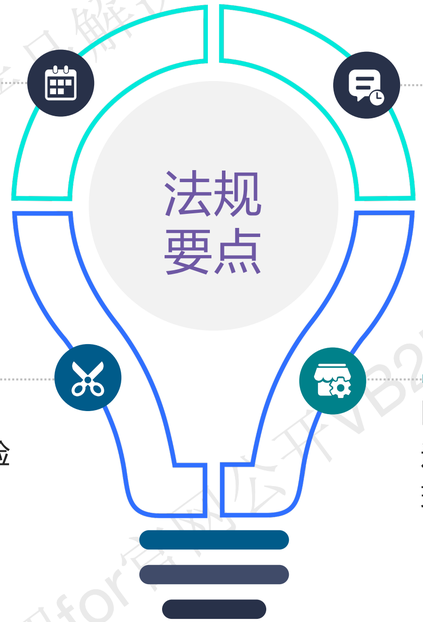
TDK MAGNA BRIDGESTONE

芯片

intel MOBILEYE NVIDIA

智能车相关软件安全重要法规标准

墨菲安全 MURPHYSEC



安全管理体系

建立车辆全生命周期信息安全管理体系、风险处置流程

漏洞管理

建立漏洞的收集、分析、处置机制

供应商风险管理

识别和管理供应链、供应商风险

产品开发全流程管理

围绕产品开发的全流程，进行风险识别、评估、管理

推荐性国家标准

GB/T 40861-2021 汽车信息安全通用技术要求

GB/T 40856-2021 车载信息交互系统信息安全技术要求及试验方法

GB/T 40855-2021 电动汽车远程服务与管理系统信息安全技术要求及试验方法

GB/T 40857-2021 汽车网关信息安全技术要求及试验方法

GB/T 41578-2022 电动汽车充电系统信息安全技术要求及试验方法

20211169-T-339 汽车诊断接口信息安全技术要求及试验方法

《关于网络安全和网络安全管理系统车辆审批的统一规定》

- 需要证明供应链 、供应商的风险已经被识别和管理
- 通过网络安全管理系统（CSMS）识别和处置漏洞

ISO/SAE 21434 道路车辆 信息安全工程

- 强调贯穿研发过程的漏洞持续监测、评估和管理

《汽车整车信息安全技术要求（征求意见稿）》

- 应建立确保对网络攻击、网络威胁和漏洞进行持续监控的流程
- 车载软件升级系统、车辆远程控制系统、授权的第三方应用等外部连接系统

应不存在由权威漏洞平台6个月前公布且未经处置的高危及以上的安全漏洞

车行业安全及合规相关严重事件

墨菲安全 MURPHYSEC

保时捷Macan由于不满足R155在欧洲停售

2023年12月，保时捷宣布最畅销的Macan车型由于不满足R155要求，2024年7月将面临3万欧元/辆的罚款，主动在2024年春季停止在欧洲售卖，成为第一个由于网络安全问题而停售的车型

丰田泄露213万辆汽车敏感数据：实时位置暴露近10年

2023年5月12日，日本丰田汽车公司承认,由于云平台系统的设置错误,其日本车主数据库在近10年间“门户大开”,约215万日本用户的车辆数据蒙受泄露风险

特斯拉遵照GPL许可证开源Autopilot

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

目录

墨菲安全
MURPHYSEC

专业、专注、可靠

智能车安全与合规挑战

墨菲安全
MURPHYSEC

合规认证挑战巨大 01

- 不同检测机构、甲方使用的检测方式不同、报告要求不一致，如何满足
- 国内外众多安全标准，对安全及合规要求极高

缺少供应商管理能力 02

- 供应商黑盒交付，缺乏手段对供应商软件的风险进行评估和管理
- 二进制软件成分分析普遍存在大量误报漏报

安全运营成本高 03

- 云、车、端资产复杂，上亿行代码、大量子系统，二进制方式部署，每天新公开上百个漏洞，分析评估成本高
- 车上相关软件涉及使用大量开源软件，存在严重的许可证合规风险

目录

墨菲安全
MURPHYSEC

专业、专注、可靠

基于标准围绕整车及软件供应商安全解决方案

墨菲安全 MURPHYSEC

贯穿车型及零部件研发流程的漏洞及许可证合规风险管理

概念设计 → 开发生产 → 测试验证 → 运营维护 → 报废下线

研发流程

软件成分分析（SCA）

- 三方代码安全漏洞/合规
- 编译产物的三方组件漏洞/合规

源安全网关

- 软件/组件选型风险评估
- 软件/组件准入安全卡位

资产管理与情报预警

- 持续监测评估云/车端资产风险

安全需求

合规认证
满足合规认证需求

供应商风险管理
动态管理供应商风险

持续安全运营
围绕产品全生命周期安全运营

合规满足

《汽车整车信息安全技术要求》

- ✓ 应建立确保对网络攻击、网络威胁和漏洞进行持续监控的流程
- ✓ 车载软件升级系统、车辆远程控制系统、授权的第三方应用等外部连接系统应不存在由权威漏洞平台6个月前公布且未经处置的高危及以上的安全漏洞

R155

- ✓ 需要证明供应链 、供应商的风险已经被识别和管理
- ✓ 通过网络安全管理系统（CSMS）识别和处置漏洞

ISO/SAE21434

- ✓ 强调贯穿研发过程的漏洞持续监测、评估和管理

四大特性 解决车安全及合规核心痛点

墨菲安全 MURPHYSEC

01 领先的供应链风险检测能力

- 针对代码片段、二进制、固件提供准确的SBOM清单识别能力
- 代码片段级的许可证风险识别及解读
- 漏洞可达性分析
- 修复兼容性评估

02 专家咨询服务保障过审查

- 对车行业相关检测及认证超10年经验安全专家团队协助解读报告、修复风险
- 为客户过认证/车企审查等专项专家支持服务，保障通过率

03 全球领先的漏洞知识库

- 全球领先的漏洞知识库，超41万漏洞库积累
- 包含准确影响组件、利用条件、PoC、触发点等40+专业漏洞字段
- 全面覆盖车联网场景的高质量漏洞库

04 专家级车企供应商交付前测试

- 熟悉国内外车企使用的各类安全检测工具
- 为整车厂的软件供应商提供专业的软件安全及开源许可证合规风险检测
- 保障通过各类国内外车企的安全审查

目录

墨菲安全
MURPHYSEC

专业、专注、可靠

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

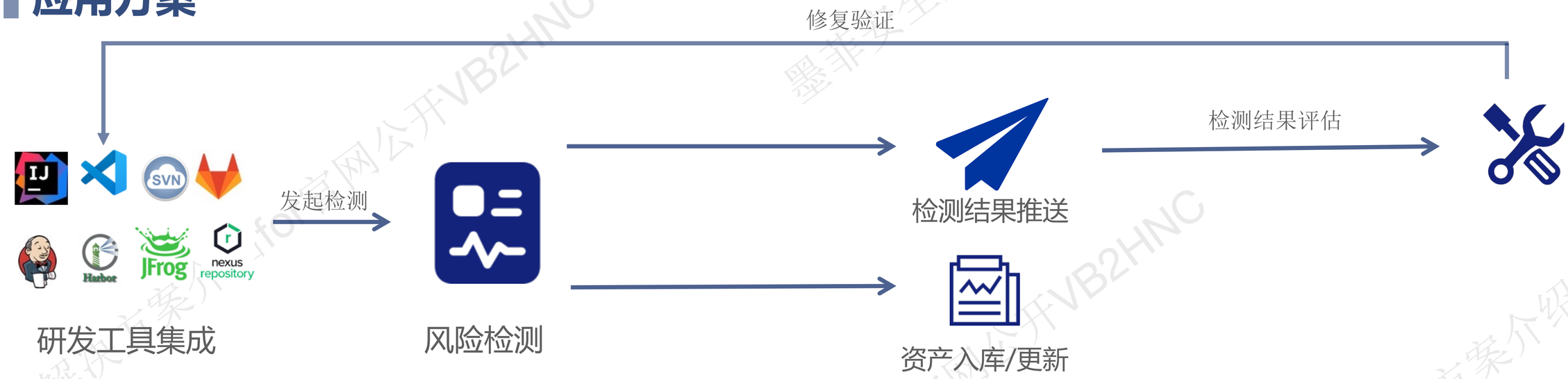
应用场景：研发过程中资产及风险管理

墨菲安全 MURPHYSEC

场景

开源漏洞频发，车端及云端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：产品交付阶段安全/许可证合规风险自查

墨菲安全 MURPHYSEC

场景

作为车企的软件/硬件供应商，整车厂将对供应商提供的软件/固件进行严格的安全/许可证合规审查

应用方案

预期效果

- ✓ 通过分析APK/固件等全面识别存在的安全漏洞及许可证合规风险
- ✓ 保障产品交付给车企客户时通过客户的安全审查

产品二：资产及漏洞情报（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

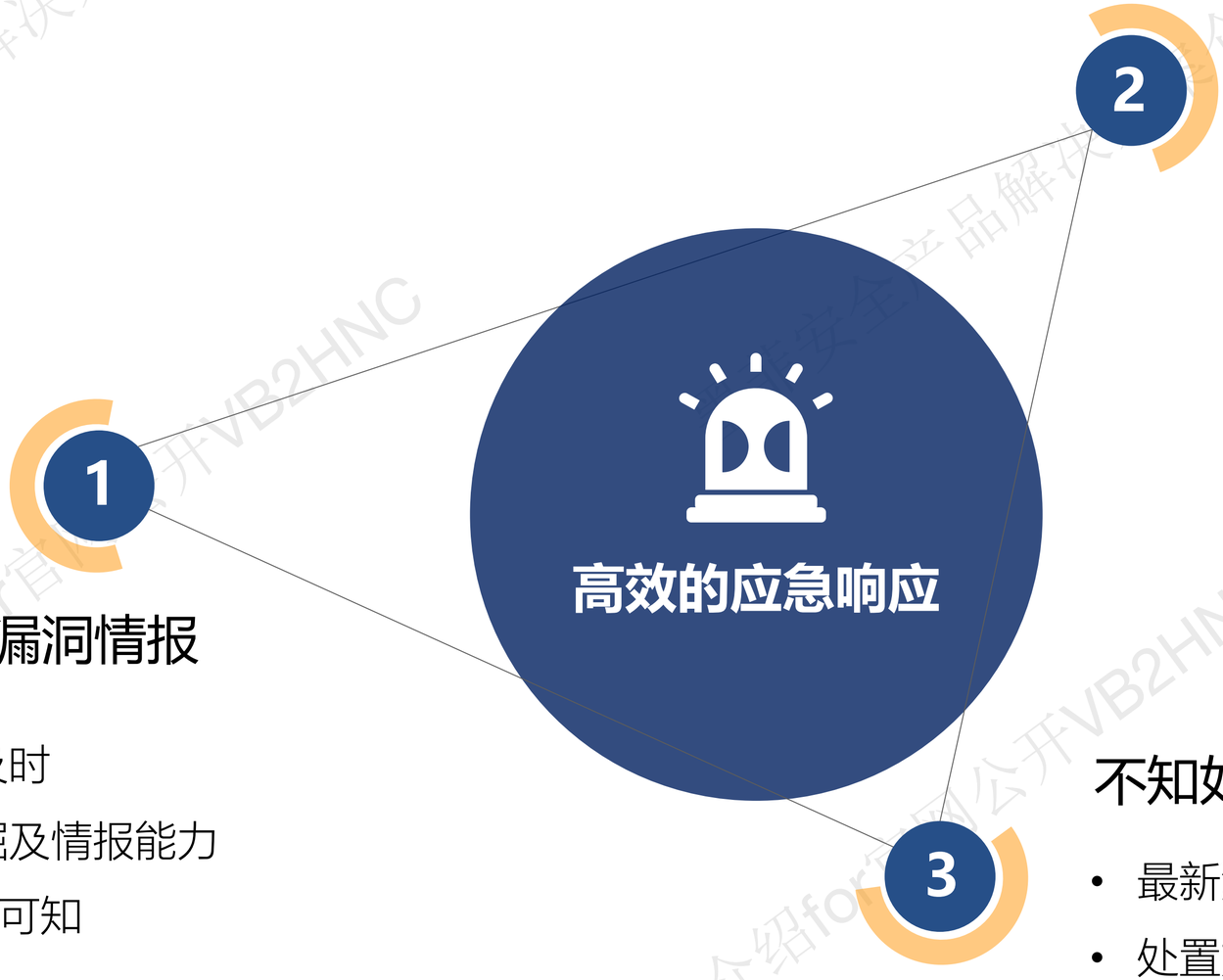
情报预警

- 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

车厂及供应商0day漏洞及投毒应急的痛点



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

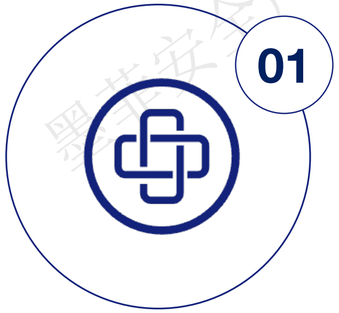
- 组件安全基线配置
- 黑白名单配置
- 支持观察模式及阻断模式
- 支持动态检测配置阻断

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

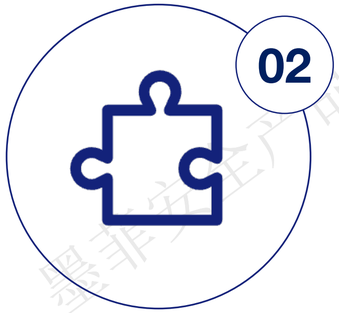
墨菲安全
MURPHYSEC



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

对含高危漏洞/许可证的开源组件进行风险拦截/审计

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


```
maven-test
[INFO] Scanning
[INFO]
[INFO] ------
[INFO] Building
[INFO] ------
Downloading f
/1.2.25/fastj
Downloaded from private-nexus: http://[redacted]:8099/repository/maven-public/com/alibaba/fastjson/
1.2.25/fastjson-1.2.25.pom (11 kB at 8.4 kB/s)
Downloading from private-nexus: http://[redacted]:8099/repository/maven-public/com/alibaba/fastjson
/1.2.25/fastjson-1.2.25.jar
[INFO] ------------------------------------------------------------------------
[INFO] BUILD FAILURE
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  1.867 s
[INFO] Finished at: 2023-08-15T21:13:58+08:00
[INFO] ------------------------------------------------------------------------
[ERROR] Failed to execute goal on project maventest: Could not resolve dependencies for project org.exam
ple:maventest:jar:1.0-SNAPSHOT: Could not transfer artifact com.alibaba:fastjson:jar:1.2.25 from/to priv
ate-nexus (http://[redacted]:8099/repository/maven-public/): transfer failed for http://[redacted]
.239:8099/repository/maven-public/com/alibaba/fastjson/1.2.25/fastjson-1.2.25.jar, status: 412 banned ->
 [Help 1]
[ERROR]
[ERROR] To see the full stack trace of the errors, re-run Maven with the -e switch.
[ERROR] Re-run Maven using the -X switch to enable full debug logging.
[ERROR]
[ERROR] For more information about the errors and possible solutions, please read the following articles
:
[ERROR] [Help 1] http://cwiki.apache.org/confluence/display/MAVEN/DependencyResolutionException
maven-test
```

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

某新势力车企L实施案例

墨菲安全
MURPHYSEC

墨菲安全产品
客户开发流程

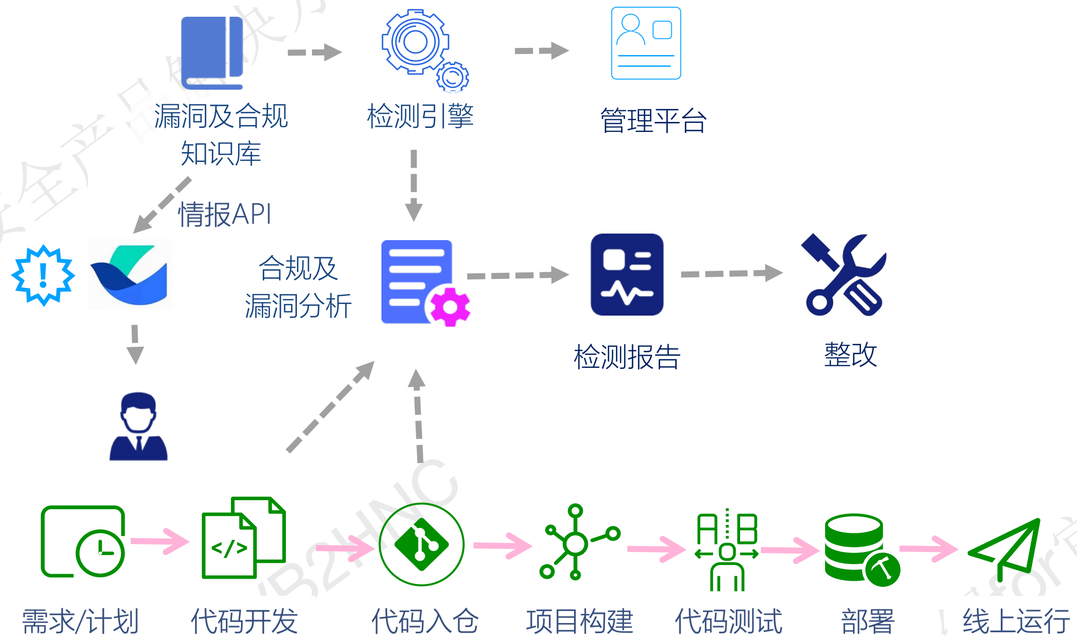
客户痛点

① 客户生产车型面向出海合规审查，担心出现风险
② 研发人员对开源许可证无法识别风险
③ 合规及数据安全要求需要加强车相关漏洞管理

挑战

① 大量C/C++代码复用导致许可证风险很大
② 大量二进制文件及固件检测成本极高
③ 云端服务使用大量开源组件，依赖关系复杂，很难准确识别

解决方案



收益

① 在开发阶段实时检测代码中调用的组件是否许可证合规
② 车线上业务代码发布之前检测完所有严重漏洞并及时修复
③ 保障对外发布产品的许可证合规

某车企供应商G实施案例

墨菲安全
MURPHYSEC

墨菲安全产品
客户开发流程

客户痛点

① 客户作为大众/宝马等车企的软件供应商，每次交付软件时被严格审查交付软件的安全及许可证合规风险

② 如果交付的软件被甲方审查发现存在安全漏洞/许可证不合规，影响交付进度及客户对产品质量的担忧

挑战

① 客户的甲方（大众/宝马等）使用的安全检测工具不一样，导致各家检测标准不一样，客户自查整改的成本巨高

② 客户交付的APK/bin固件的人工安全测试难度大，经常覆盖不全导致交付时漏掉安全风险及许可证合规

解决方案

收益

① 每次打包发布后的apk/bin固件顺利交付，获得客户验收及好评

② 大大降低安全人员审查的成本及效率

墨菲安全

目录

墨菲安全
MURPHYSEC

专业、专注、可靠

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/