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

资产管理及漏洞&投毒情报预警

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；

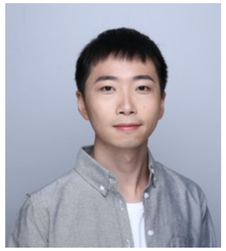
产品技术领先 顶级的漏洞研究及应用安全实践经验，创始人曾在乌云主导国内首款检测SaaS产品TangScan；

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

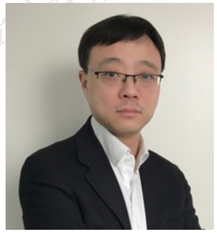


联创&实验室负责人 欧阳强斌

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　中国建筑 CHINA STATE CONSTRUCTION　理想

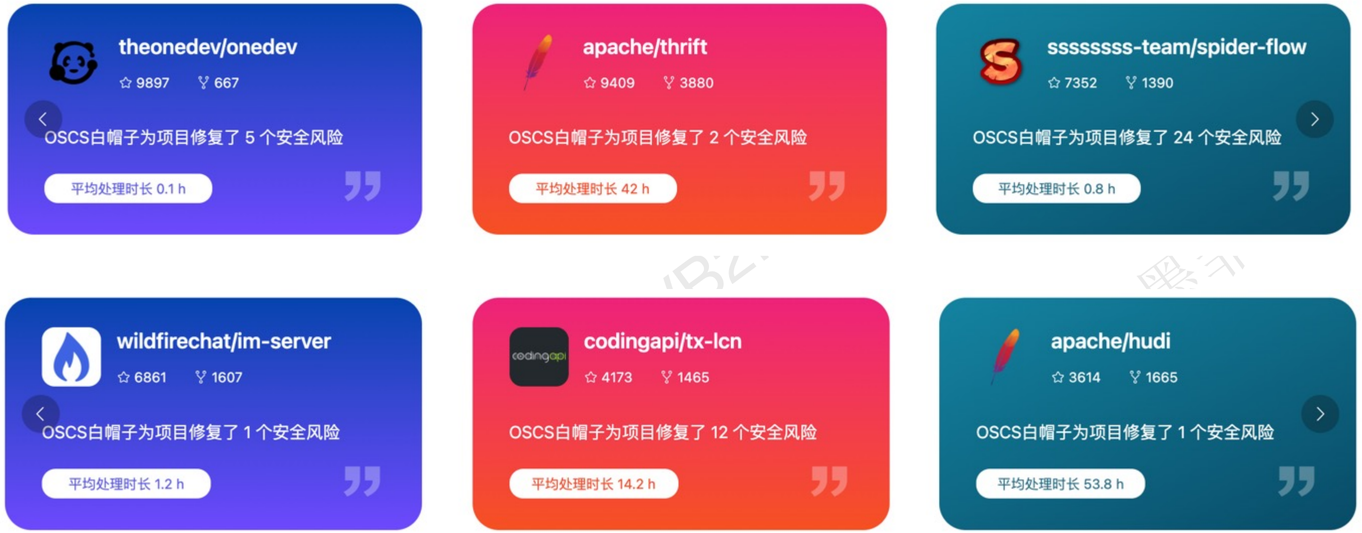
监管合作

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

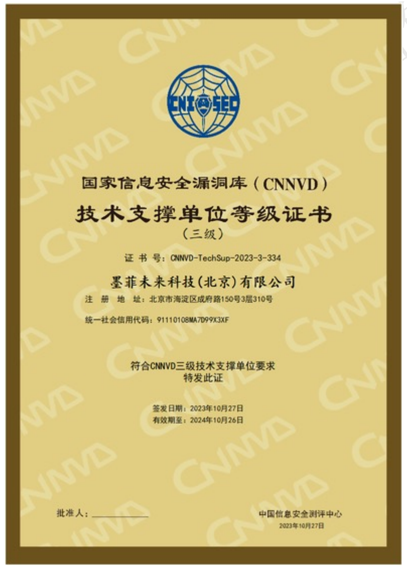
750万 累计发现漏洞数

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

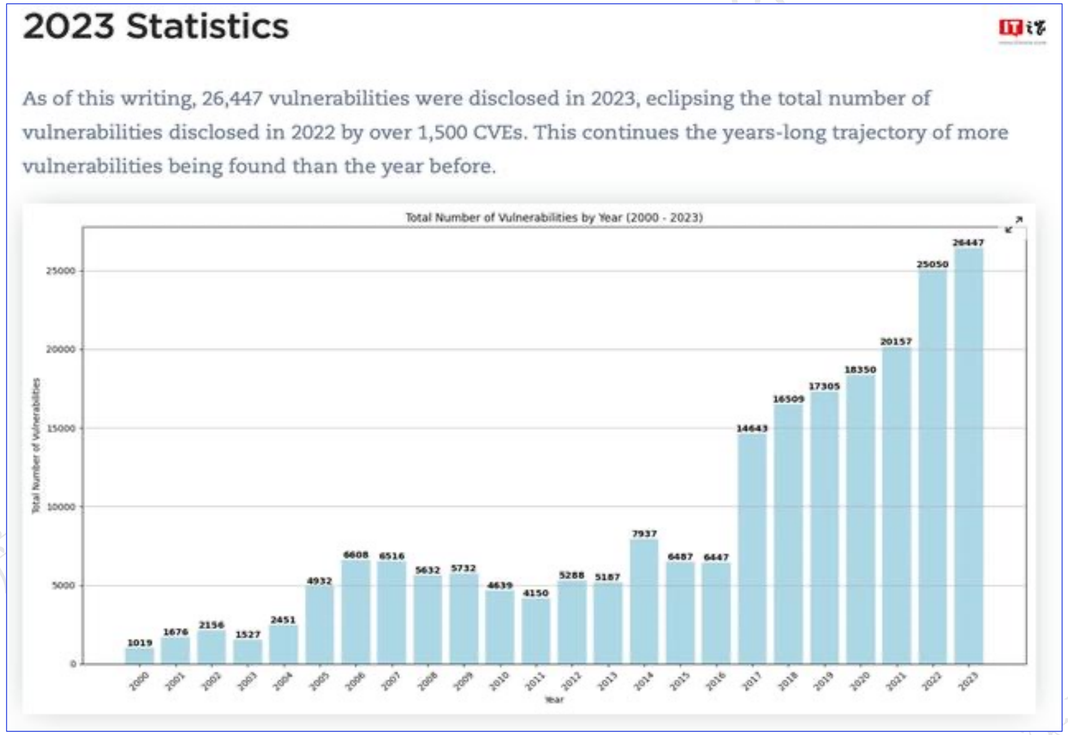
供应链软件0day漏洞及投毒已成为企业主要威胁

墨菲安全 MURPHYSEC

25% 高风险漏洞在发布当天被利用，2023年恶意软件包为2022年 **3倍**，投毒攻击已成为下一代供应链攻击主要方式

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， **25%的高风险漏洞**在发布当天就被利用

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。



注：数据来源为Sonatyoe，第九届软件供应链安全报告

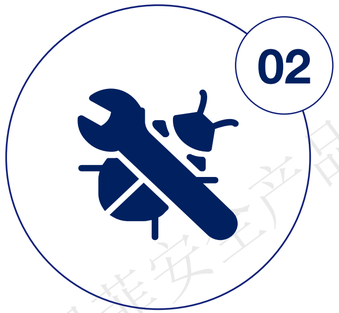
供应链0day漏洞是企业威胁最大的黑天鹅事件

墨菲安全
MURPHYSEC

01

不可预测性

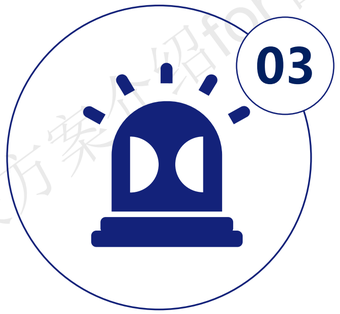
- 0day漏洞曝光前都是不可预测的
- 任何软件随时都可能被发现高危0day漏洞



02

高危害性

- 0day漏洞往往影响广且易造成企业数据泄露/加密勒索等
- 往往企业使用的越广泛的软件越容易被发现0day



03

极大利益驱动

- 全球最知名的加密勒索团伙使用的都是供应链软件0day/1day漏洞
- 全球网络黑产/政治势力/恶意商业竞争背后使用的核心武器几乎都是软件供应链0day漏洞

04

没有防御准备

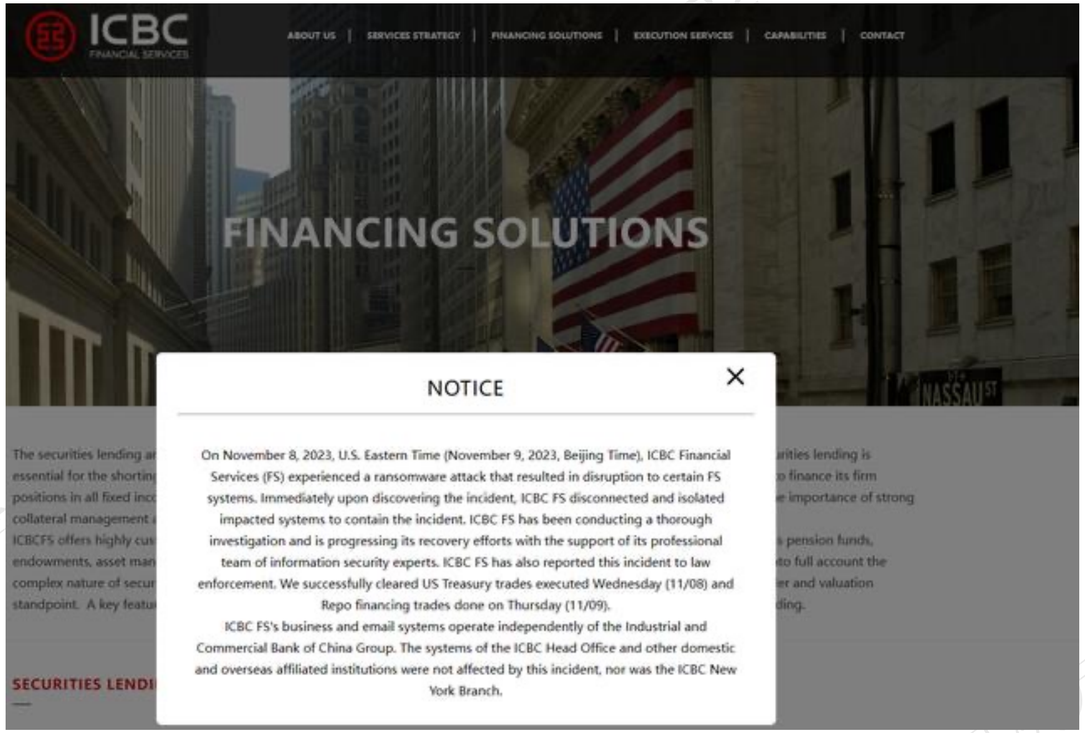
- 因为是不可预测的，所以企业根本无法防范
- 企业已知的防护手段都无法应用于0day的漏洞防护

典型的软件供应链0day漏洞攻击事件

墨菲安全 MURPHYSEC

工行美国子公司因0day漏洞遭遇勒索软件攻击

美东时间11月8日，工行在美全资子公司ICBCFS在声明中提到，“由于遭勒索软件攻击，导致部分系统中断，目前工行已支付赎金；
此次攻击来自Lockbit勒索软件组织，利用的是工行美国子公司使用的供应链软件Citrix的一个0day漏洞；



OpenAI 因redis组件库漏洞导致用户数据泄露

3月24日，OpenAI发布报告称Redis客户端开源库redis-py中存在漏洞，引发ChatGPT暴露了其他用户的聊天会话查询和个人信息，大约有1.2%的ChatGPT Plus订阅用户受到影响。暴露的信息包括订阅用户姓名、邮件地址、支付地址、信用卡后四位数字和信用卡过期日期。

典型软件供应链0day漏洞及投毒攻击事件

墨菲安全 MURPHYSEC

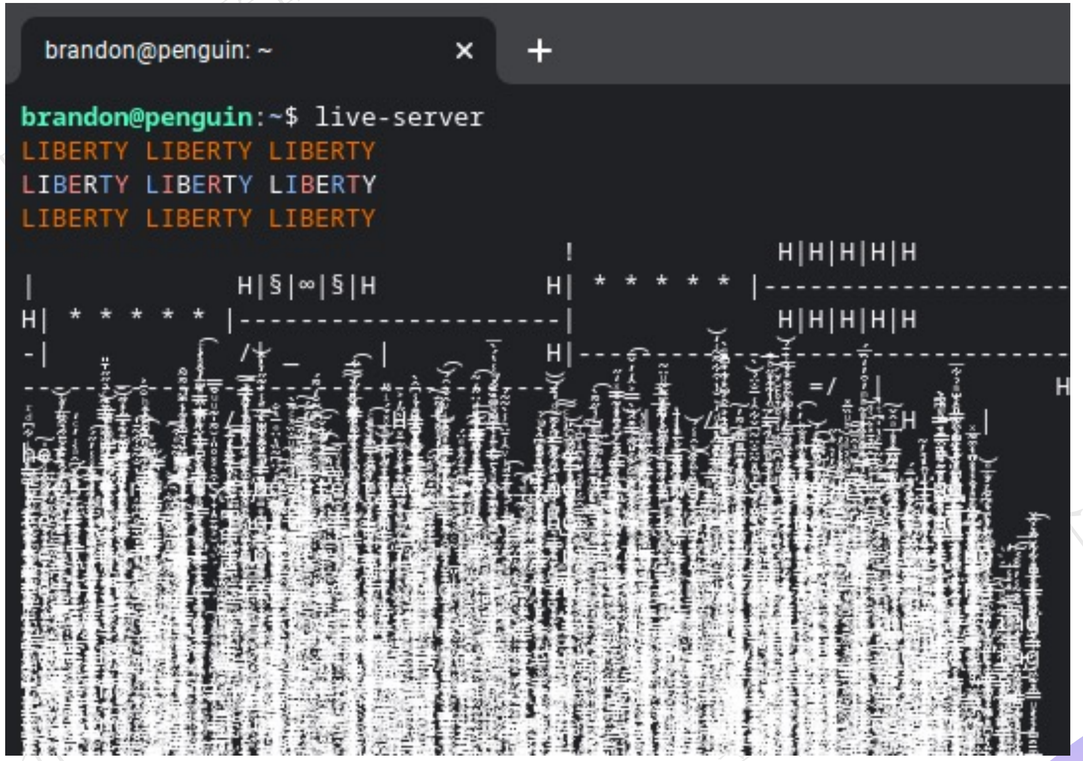
Log4j爆出严重漏洞影响全球65%企业

log4j漏洞公开第二天，国内多家企业SRC由于收到大量漏洞报告而暂停接收该漏洞

自2021年12月15日以来的Log4j总下载量 **249, 556, 989次**，其中 **29%** 为易受攻击版本，全球 **65%** 的企业受该漏洞影响

faker.js、colors.js事件

该开源组件作者由于不满用户免费使用，加入恶意代码，使用户执行后会输出三行「LIBERTY LIBERTY LIBERTY」，而后开始无限输出非 ASCII 字符



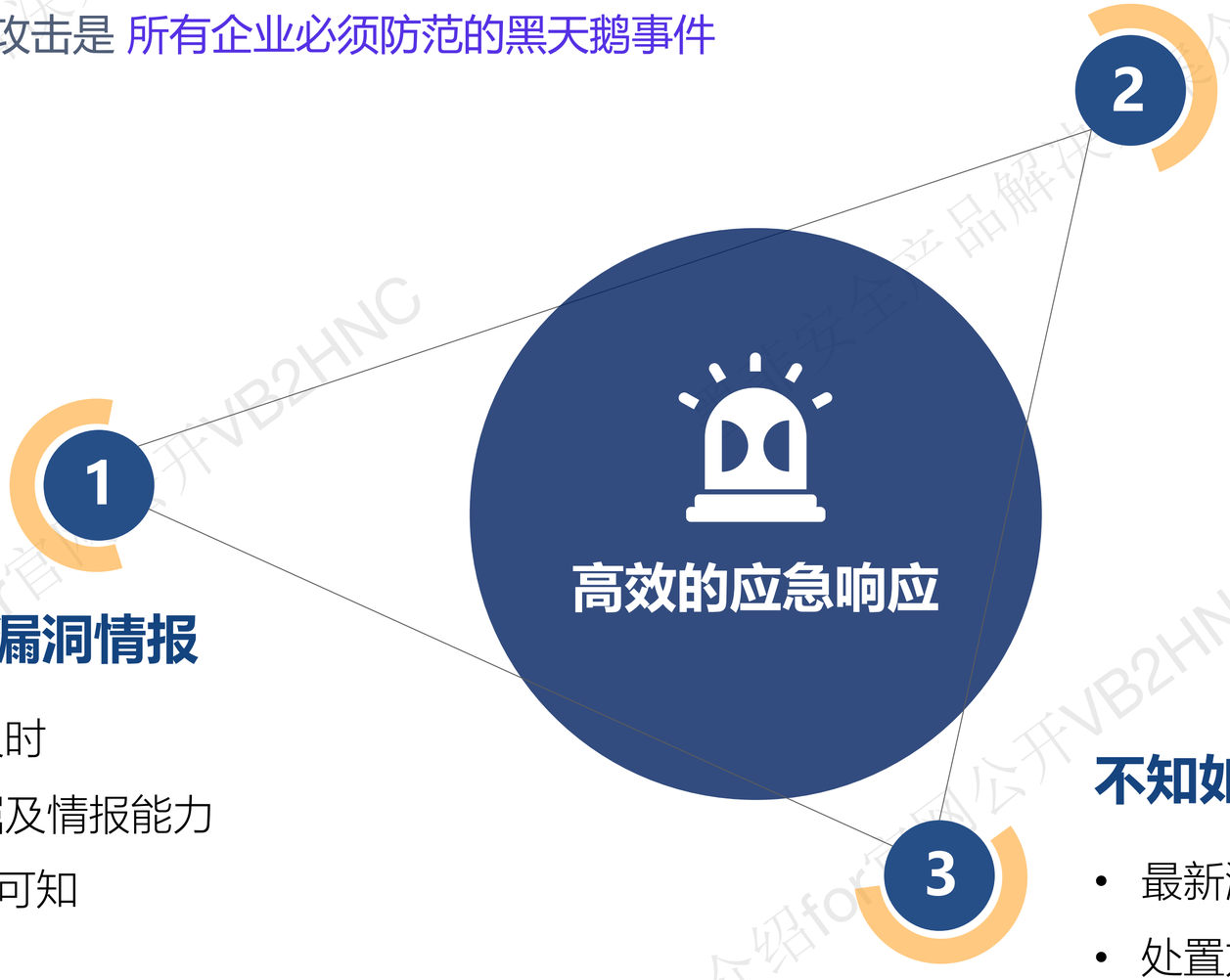
目录

墨菲安全
MURPHYSEC

专业、专注、可靠

企业应对突发0day漏洞及投毒攻击的三大挑战

突发0day漏洞及投毒攻击是 所有企业必须防范的黑天鹅事件



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
- 资产和最新漏洞关键不起来

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

目录

墨菲安全
MURPHYSEC

专业、专注、可靠

围绕 资产 + 情报 打造高效的应急处置方案

墨菲安全 MURPHYSEC

应用场景

应急响应

- 情报预警
- 关联资产
- 事件告警
- 应急处置

安全能力提升

- 0day分析报告
- SAST/SCA/IAST/DAST 添加规则
- 生成规则
- WAF/IDS/IPS/HIDS 添加规则

墨菲产品能力

资产管理及漏洞&投毒预警平台

- 软件供应链资产台账
  - 商业软件
  - 开源/免费软件
  - 自研web应用
  - 自研移动应用
- SBOM
- 软件成分分析引擎

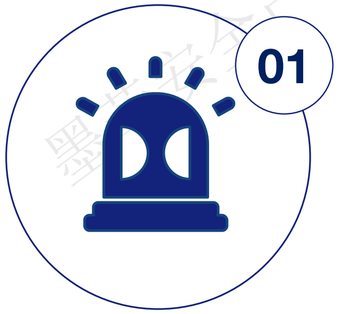
+

- 0day漏洞&投毒情报预警
  - 漏洞基础信息
  - 25+独有字段
  - 详细分析报告
  - 指纹信息
  - 开源组件漏洞情报
  - 开源组件投毒情报
  - 商业软件漏洞情报

- 服务器
- 办公电脑
- 代码仓库
- 容器镜像仓库
- 私有源

四大特性 解决应急响应核心痛点

墨菲安全
MURPHYSEC

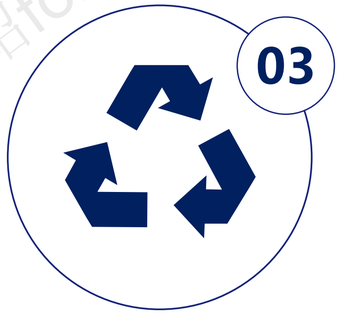


01 及时有效的漏洞&投毒情报

- 超100类监控渠道，获取一手漏洞信息
- 独家0day漏洞&投毒情报挖掘覆盖
- 超过90%漏洞情报推送早于友商

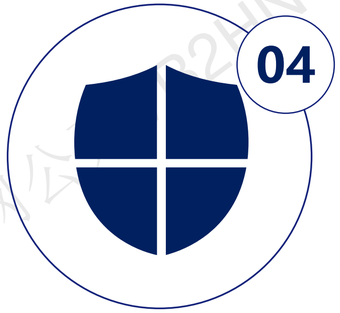
02 精准详细的高价值漏洞信息

- 策略+AI+专家体系化运营
- 超25项独家高价值字段，含POC/漏洞触发点/真实影响/指纹等
- 100%可信保障，可落地的漏洞处置方案



03 漏洞影响反馈快速排查

- 极低成本采集&管理应用资产
- 漏洞影响范围资产自动关联
- 安全事件单实时推送



04 极速提升安全防护能力

- 支撑快速添加WAF/IDS/xAST规则
- 组件坐标排查方案
- 指纹排查方案
- 进程排查方案

目录

墨菲安全
MURPHYSEC

专业、专注、可靠

资产管理及漏洞&投毒情报（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

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

安全赋能

- WAF/IDS/xAST规则
- 组件坐标排查方案
- 进程排查方案
- 指纹排查方案

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！

某头部金融客户M实施案例

墨菲安全 MURPHYSEC

客户痛点

① 0day漏洞响应及时度不够，处置成本高，容易导致被攻击

② 客户对软件供应链安全防护要求极高，对漏洞知识库及情报的时效性和准确的要求极高，自有人力维护困难

挑战

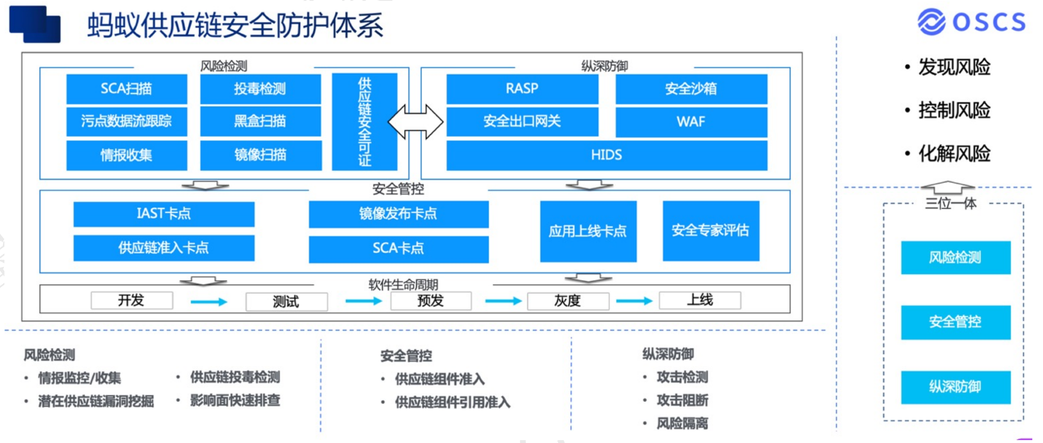
① 每天外部曝出的0day漏洞太多，跟不过来，不跟进又怕漏掉

② 大量CVE漏洞无法判定其真实影响

③ 大量CVE漏洞的基础信息不完备且不准确，无法响应和处置

解决方案

墨菲的漏洞&投毒情报及知识库支撑蚂蚁集团完善软件供应链安全防护体系



收益

① 0day漏洞及投毒情报的响应效率大幅提升，自有人力投入大幅下降

② 帮助客户集团的软件供应链安全体系从1.0提升到3.0阶段

蚂蚁集团 ANT GROUP 蚂蚁集团网络安全副总经理 程岩

软件供应链威胁，其攻击门槛低、影响范围广、攻击方式隐蔽、危害大，且近年来攻击事件持续高发，已成为最具影响力的高级威胁之一。同时，当下被公开的攻击事件只是冰山一角，冰山之下更是大量软件供应链从未公开披露漏洞和被投毒事件。蚂蚁集团长期持续建设和演化供应链安全体系，从1.0 十万火急，走过2.0 游刃有余，已进入3.0 持续可信阶段，对内部自研和外部供应商都提出极高的标准和指标要求。墨菲安全是我们在供应链安全领域引入的唯一外部技术供应商，其为我们提供了一套成熟、厚重和持续迭代的供应链安全知识和情报信息，为我们构建3.0体系提供了强有力的能力和服务支撑。在合作的一年多时间里我们深刻体会到墨菲安全不管是在技术深度还是在产品服务体验上都表现的非常专业。

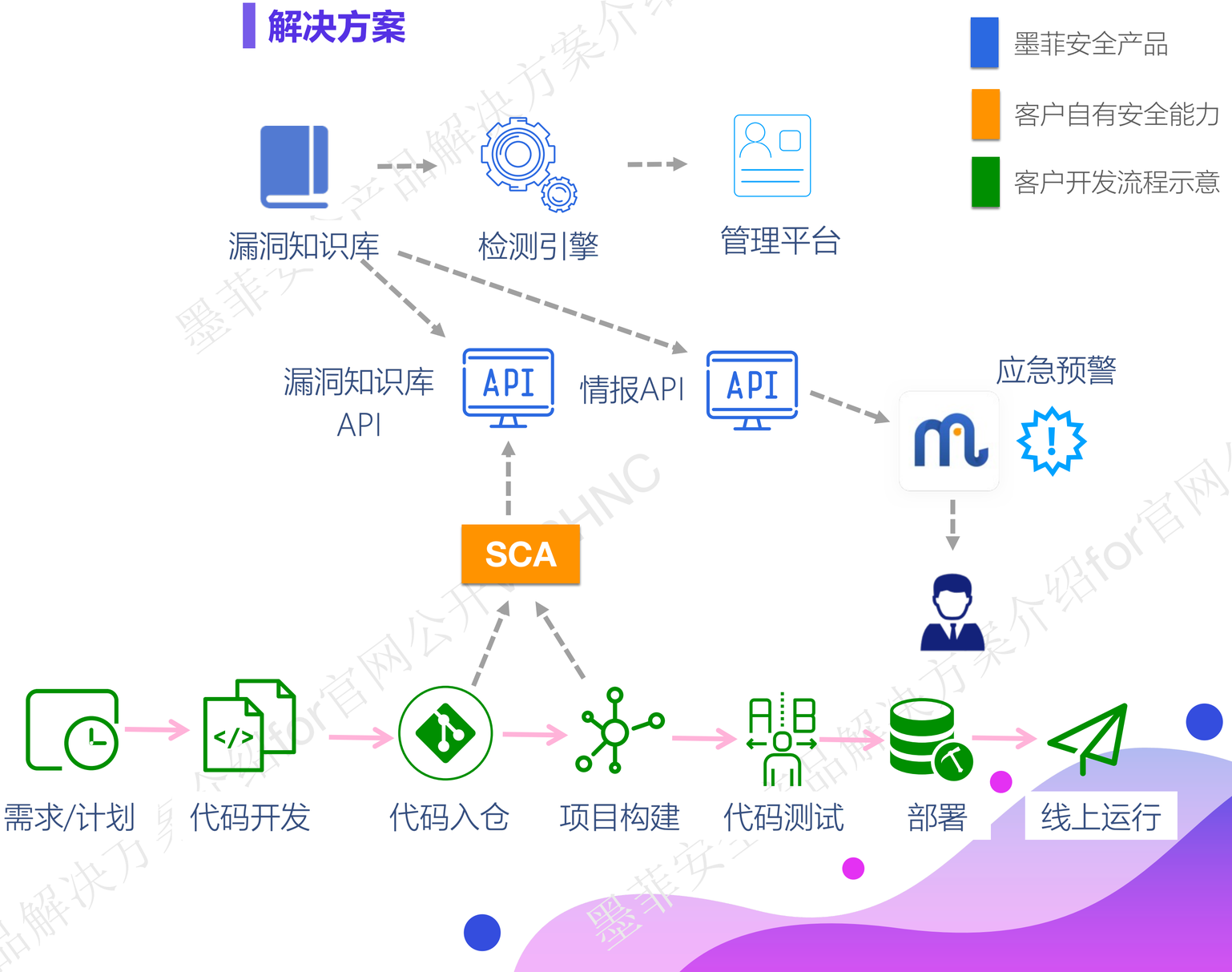
某互联网客户M实施案例

墨菲安全
MURPHYSEC

客户痛点

① 基础架构部门开发了SCA，漏洞库需要安全支持
② 安全部门维护漏洞知识库成本高，效果不佳
③ 0day漏洞响应及时度不够，处置成本高

解决方案



收益

✓ 安全部门为基础架构部门提供优质的漏洞知识库
✓ 安全部门0day漏洞应急处置效率提升60%

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/