基于社区的企业安全管理

火线安全 联合创始人 卢中阳

luzhongyang@huoxian.cn

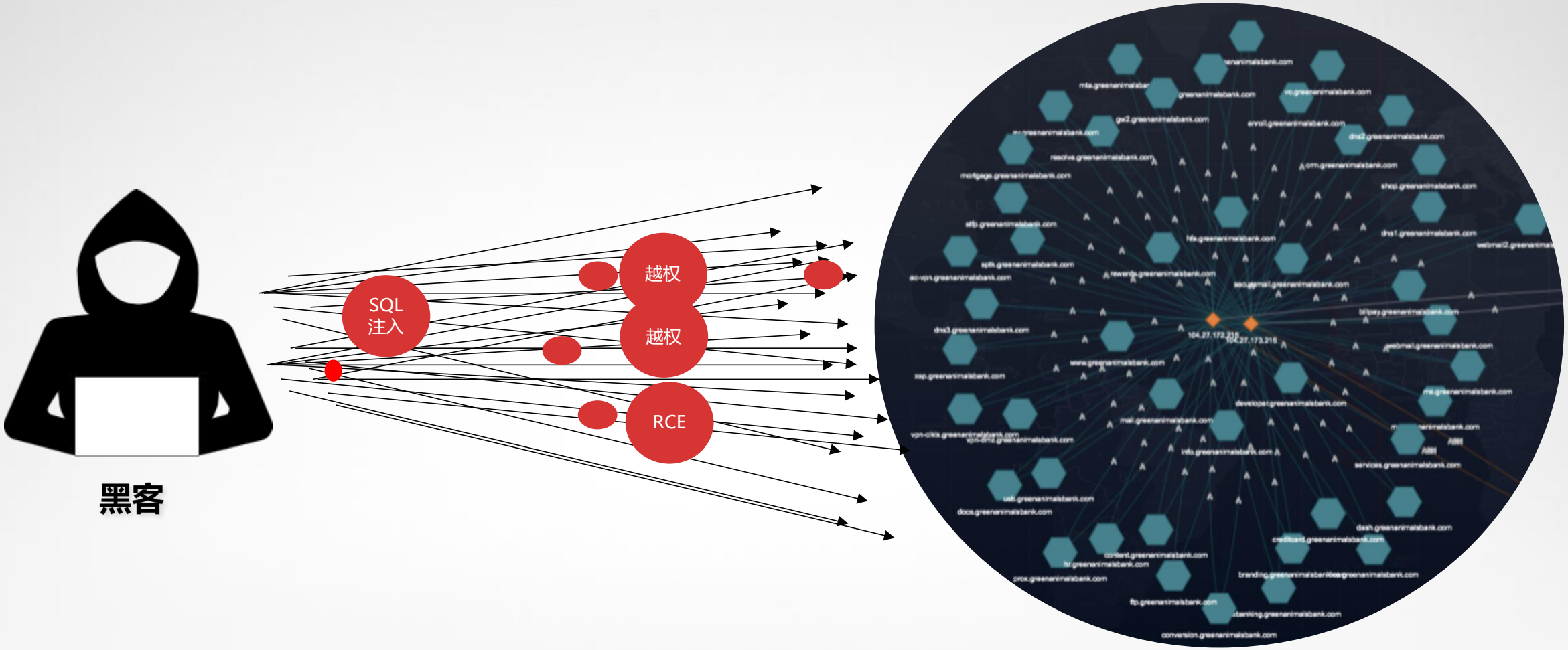
火线

目录 *Contents*

风险 来自于哪里

Where does the risk come from

漏洞 = 漏洞知识库+暴露资产



一切皆为资产，管理难度大

Restful、GraphQL、RPC、Tomcat、Android、IOS、IOT、 Spring Boot、 Dubbo...
MySQL、Oracle、Redis、 Kafka、 ActiveMQ、Zabbix、Jenkins、F5 Linux、Windows、 vSphere、ESXi、k8s、Harbor

Github、Gitlab、Coding、阿里云效、码云、百度网盘、百度文库、数据论坛、语雀、confluence、暗网论坛

FeiQ、QQ、微信、钉钉、飞书、Exchange、Coremail、腾讯企业邮、Gmail、致远OA、CISCO SSL VPN

业务应用

- API接口
- 中间件
- 客户端软件
- 开源组件
- 微服务
- Serverless

运维服务

- 数据库
- 消息中间件
- 可视化运维
- RDS
- SLB

基础环境

- 操作系统
- 虚拟机
- Kubernetes
- 镜像仓库
- AWS、aliyun、腾讯云

数据管理

- 业务代码
- 业务数据
- 密码凭证
- 内部资料

办公系统

- IM系统
- 邮件系统
- OA系统
- VPN系统

供应链

- 采购系统
- 客服系统
- 招聘系统
- 销售系统

企业互联网攻击面

火线

资产管理难度越来越大

传统资产多云化

传统IDS+办公网+公有云+私有云

资产边界宽泛化

IP、域名、接口、容器、组件、账号、秘钥、云服务、业务云服务

资产管理方式复杂化

CMDB、流量分析、主机监控、黑盒监控

火线

社区众测中常见的漏洞分类

漏洞监控 CVE、CNNVD、CNVD Github、exploitdb、安全社区

业务逻辑

账号逻辑
支付逻辑
权限体系
数据重放
消耗攻击
弱密码问题

接口安全

SQL注入
SSRF
反序列化
XSS漏洞
文件上传
组件漏洞
任意命令执行

运维服务

服务未授权
服务弱密码
服务配置不当
服务软件漏洞

基础环境

弱密码
配置不当
环境未隔离
密钥泄漏
容器权限提升
OSS配置错误

安全意识

代码泄漏
文档泄漏
凭证泄漏

社区漏洞分布

云化过程带来

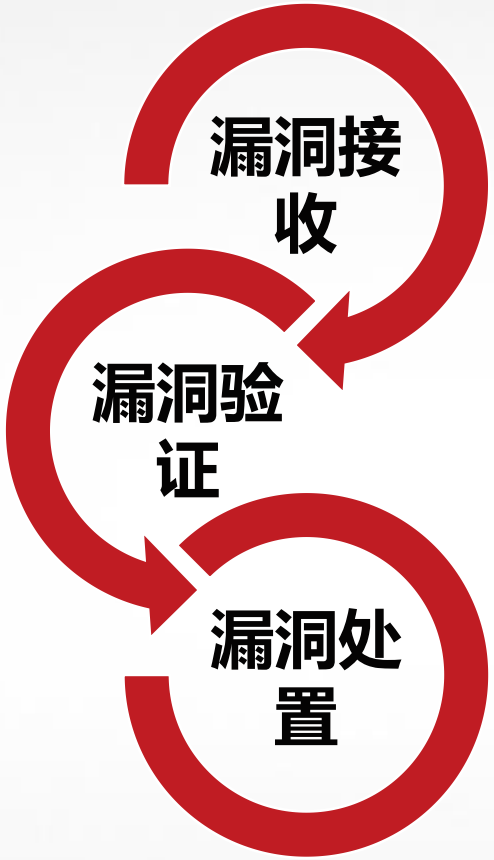
更多新型漏洞攻击

漏洞频发

监控难度大

线上的漏洞成本逐渐增高

1. 渗透测试
2. 攻防演习
3. 漏洞扫描
4. 漏洞通报



1. 有效性验证
2. 漏洞分级
3. 漏洞影响评估

1. 修复建议
2. 工单处置
3. 漏洞复测

运营成本持续增高

线上安全测试服务思考

1. 安全测试按人天等收费是否合理
2. 如何保证测试效果
3. 如何保障漏洞安全
4. 如何高效的进行安全测试

基于社区的安全风险管理

火线安全的漏洞闭环解决方案

兜底查漏

互联网众测模式的
漏洞快速收敛

资产梳理

社区资源分配

协同赋能

漏洞管理

策略运营

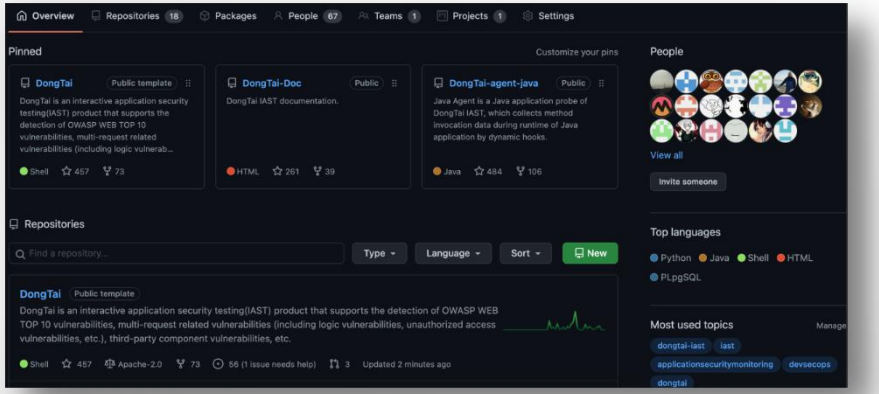
能力沉淀

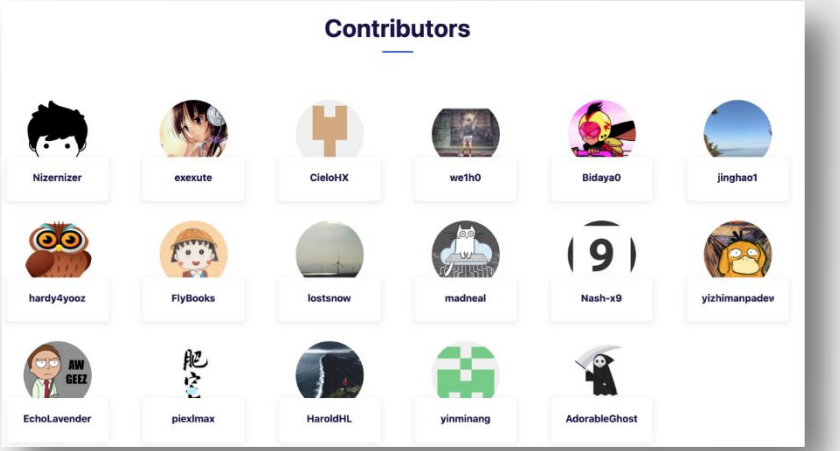
持续检测

漏洞管理

基于DevSecOps可
持续的漏洞持续运营

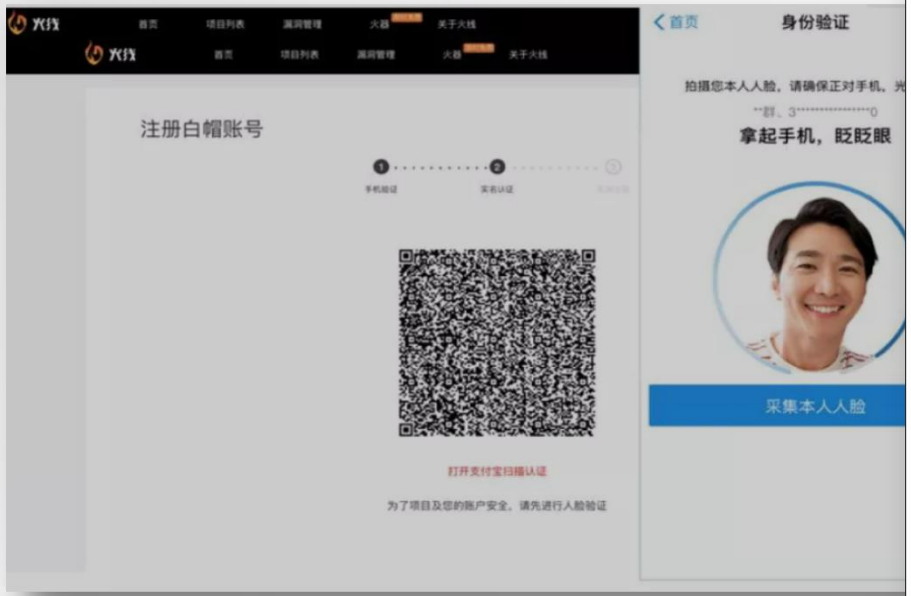
复盘沉淀

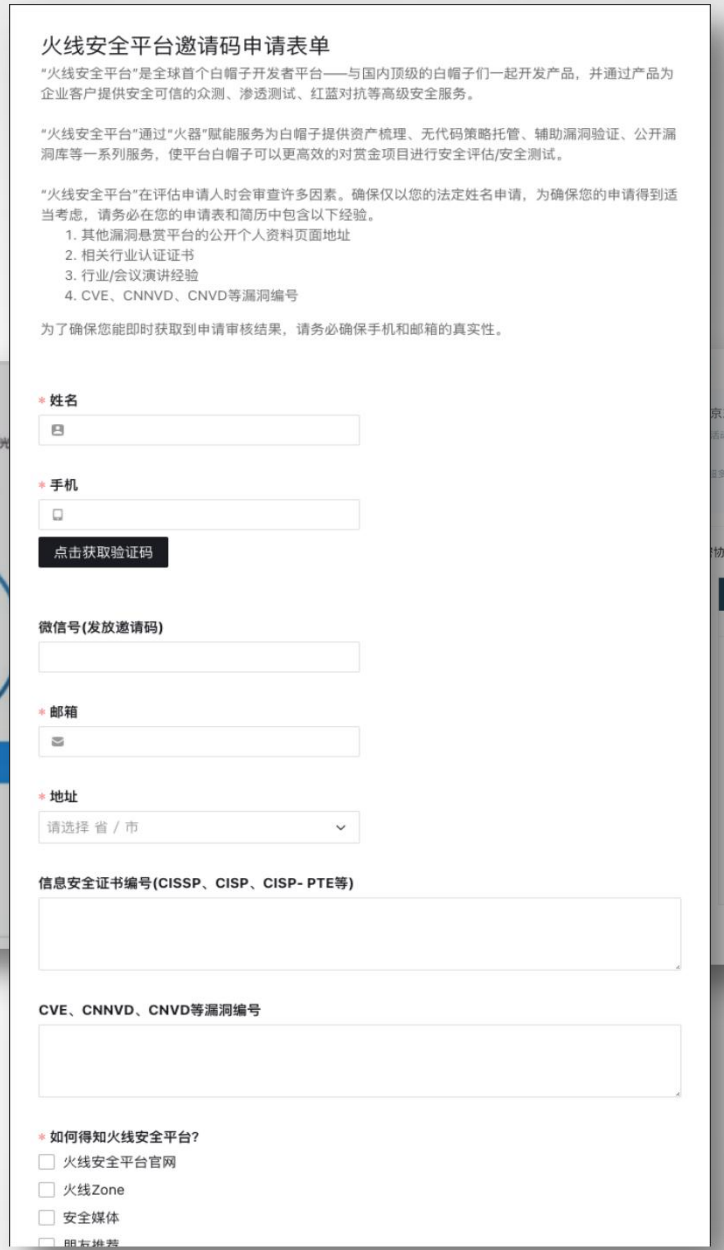




可信的白帽社区

1. 封闭邀请审核准入制度
2. 强实名人脸认证
3. 多重保密协议在线签约





强大的社区数据资源支持

企查查 Qcc.com

工业和信息化部政务服务平台 ICP/IP地址/域名信息备案管理系统

ChinaZ.com China Webmaster 站长之家

hunter

天眼查 TianYanCha.com

crt.sh Certificate Search

WhoIs

腾讯应用宝

Google

Bing

ipinfo.io

西瓜数据 DATA.XIGUAJI.COM

Baidu 百度

Github

资产收集

百度网盘

Baidu 文库

FOFA

ZoomEye

HACKER TARGET

censys

OpenDNS

VIRUSTOTAL

NMAP.ORG

MASSCAN MASS IP PORT SCANNER

ThreatBook 微步在线

Layer子域名挖掘机

OneForAll

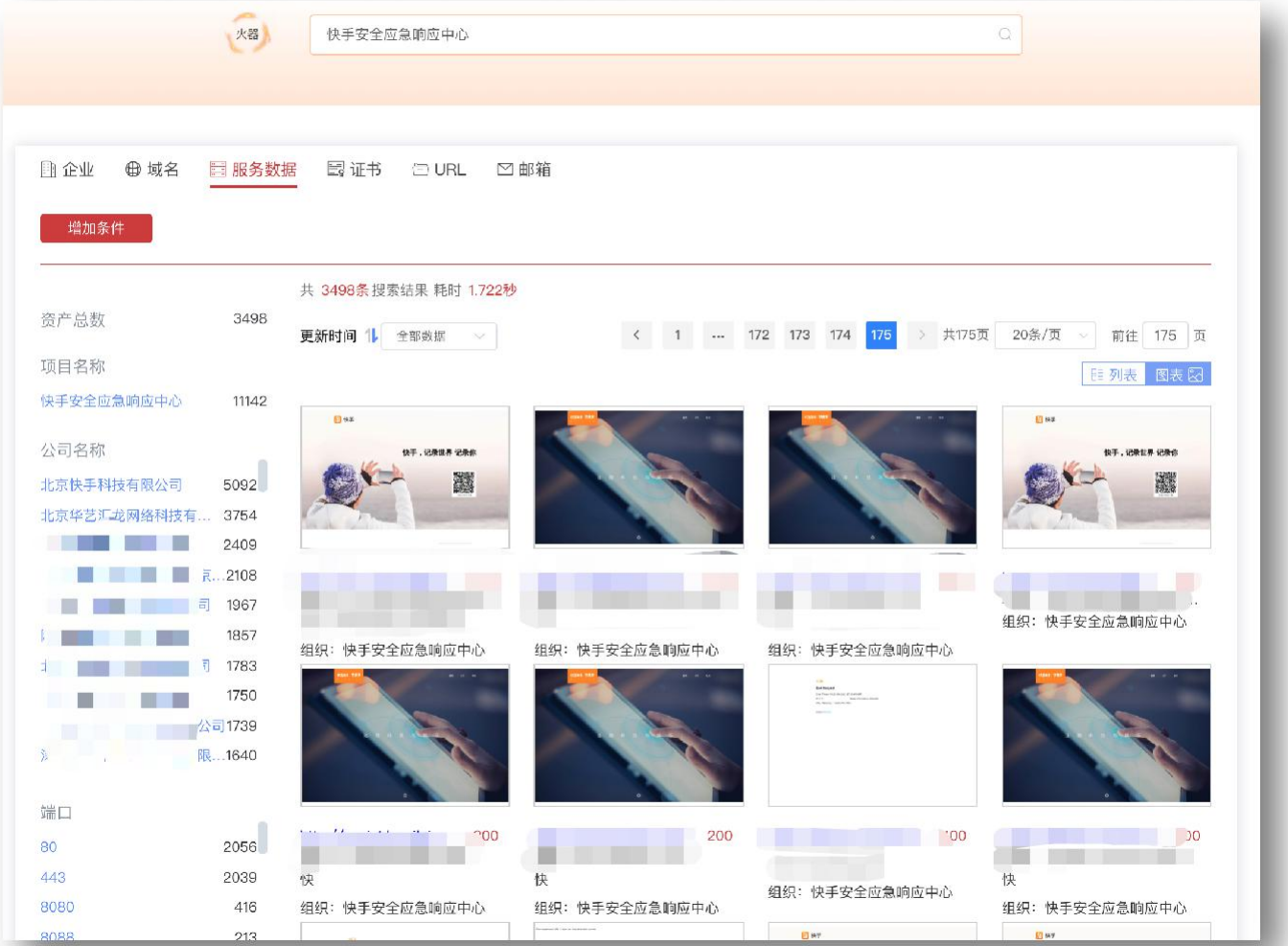
subDomainsBrute

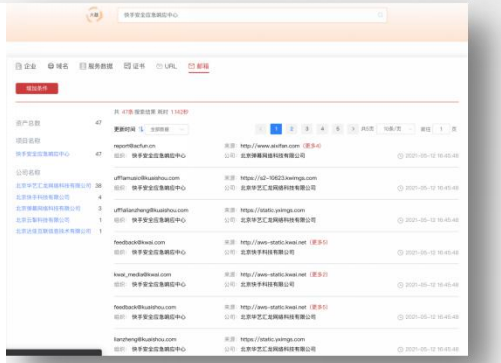
Wappalyzer

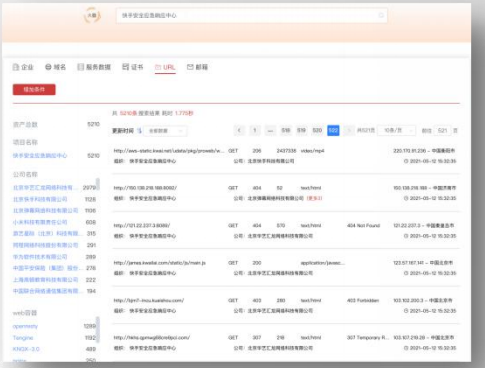
云悉 yunsee.cn

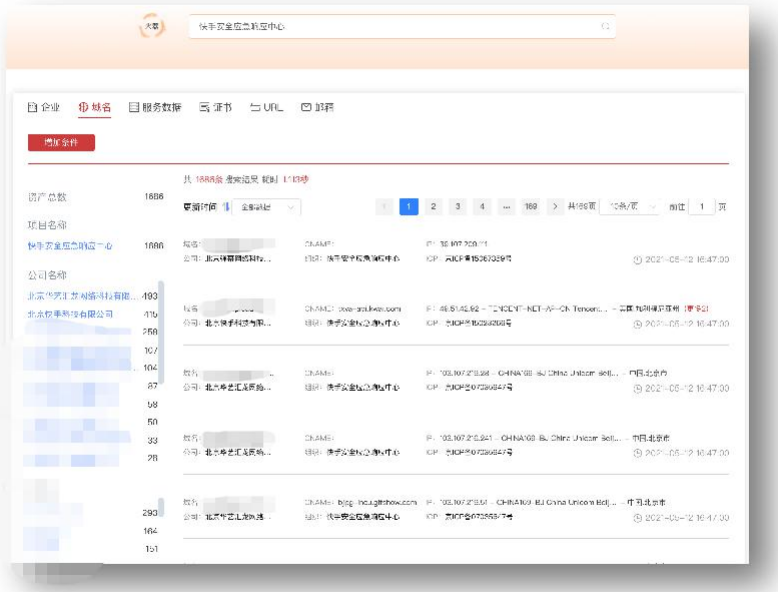
8000万Whois数据	500万ICP数据	1800万域名解析数据	43亿IP定位数据
50亿证书数据	1000万URL数据	170万APP应用数据	2800万邮箱数据

强大的社区数据资源支持

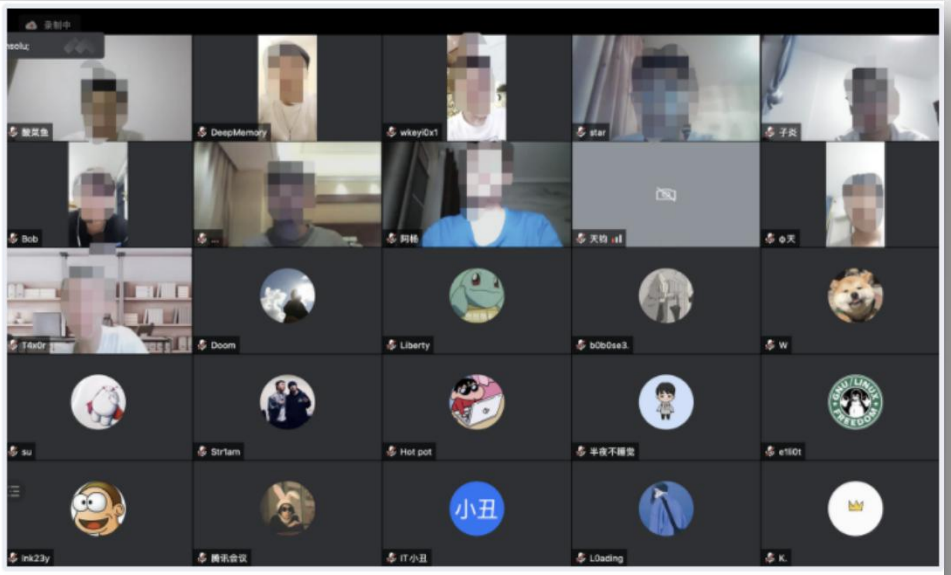




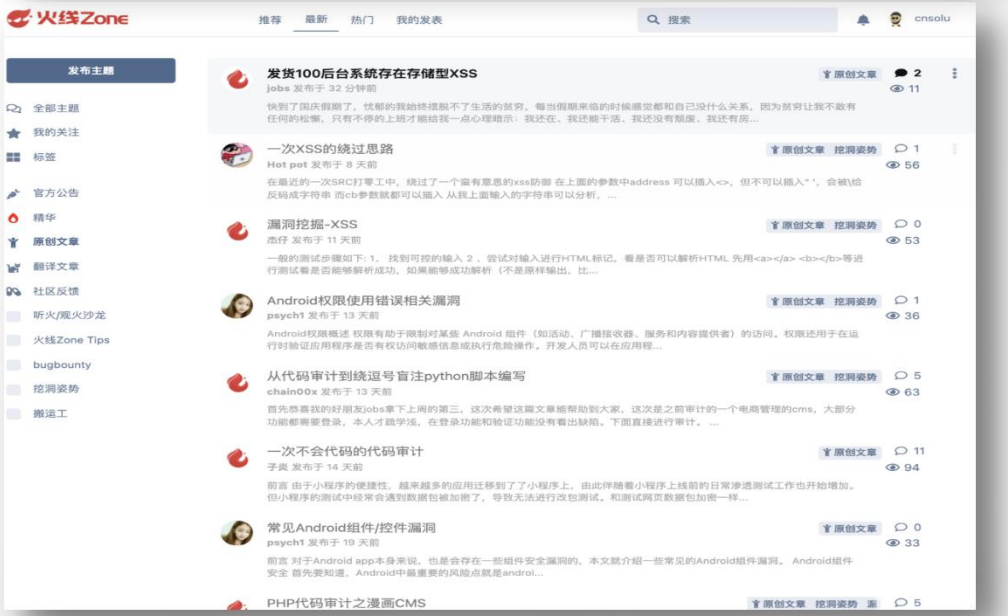




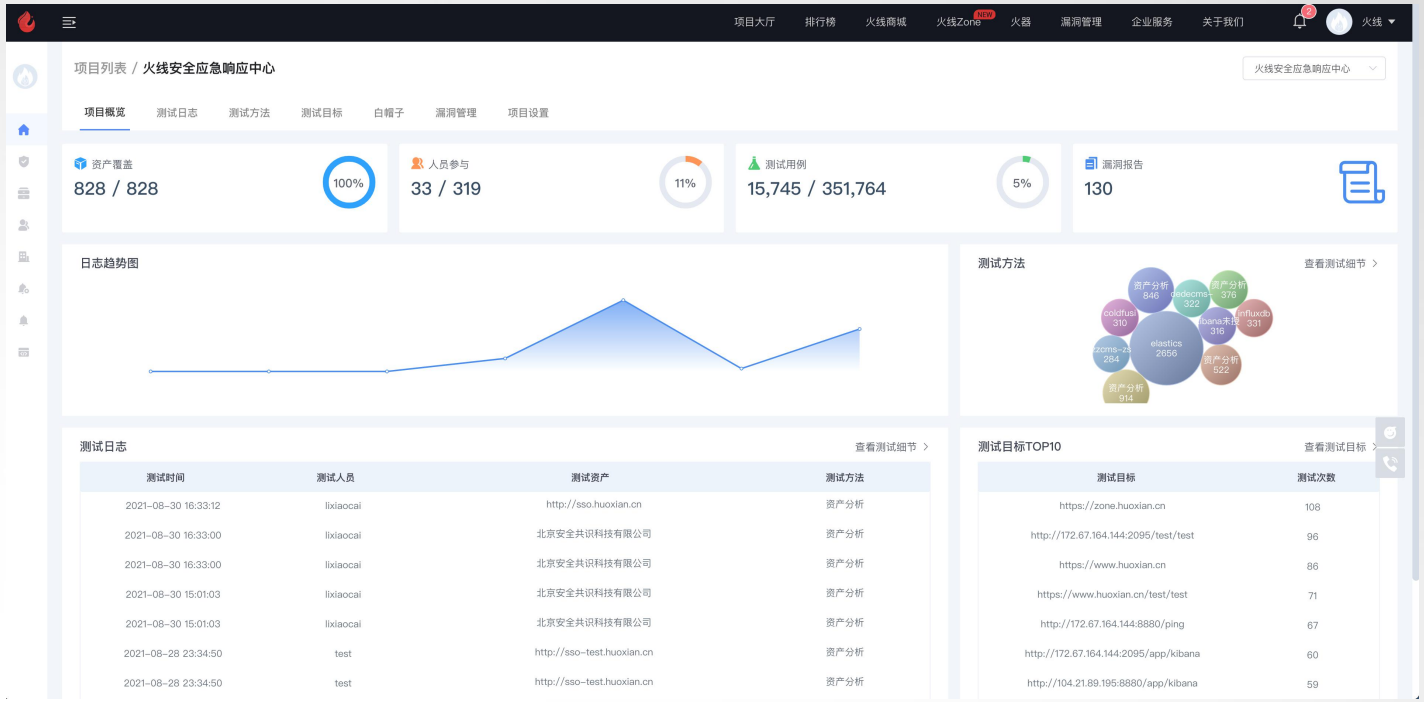
社区知识共享，稳定的技术输出



漏洞分享片段

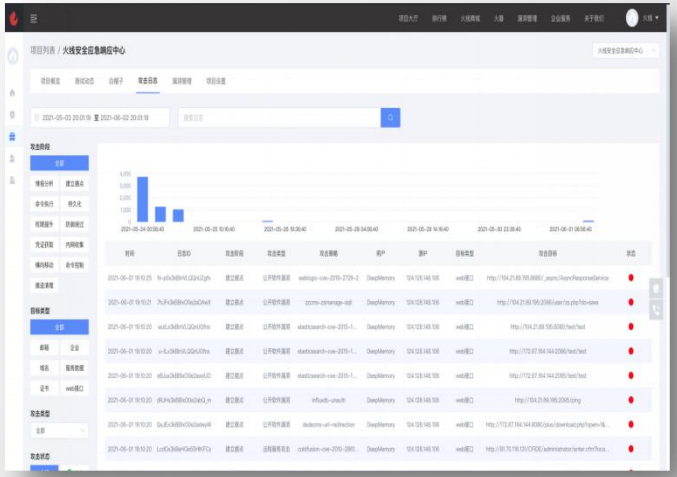


可视化的测试管控

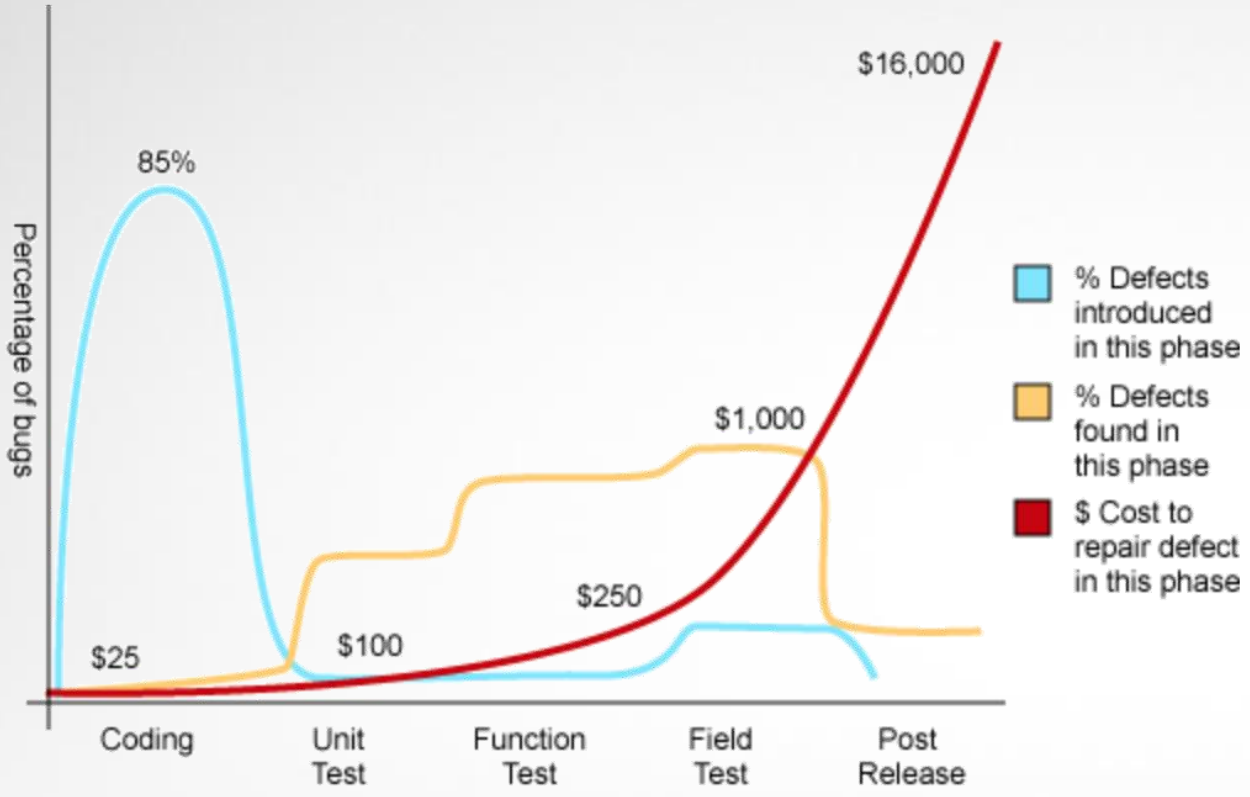


丰富的第三方集成

- ✓ 企业微信
- ✓ 钉钉
- ✓ 飞书
- ✓ 微信公众号
- ✓ 短信
- ✓ 邮件
- ✓ OpenAPI
- ✓ WebHook



软件上线后修复成本成倍增加

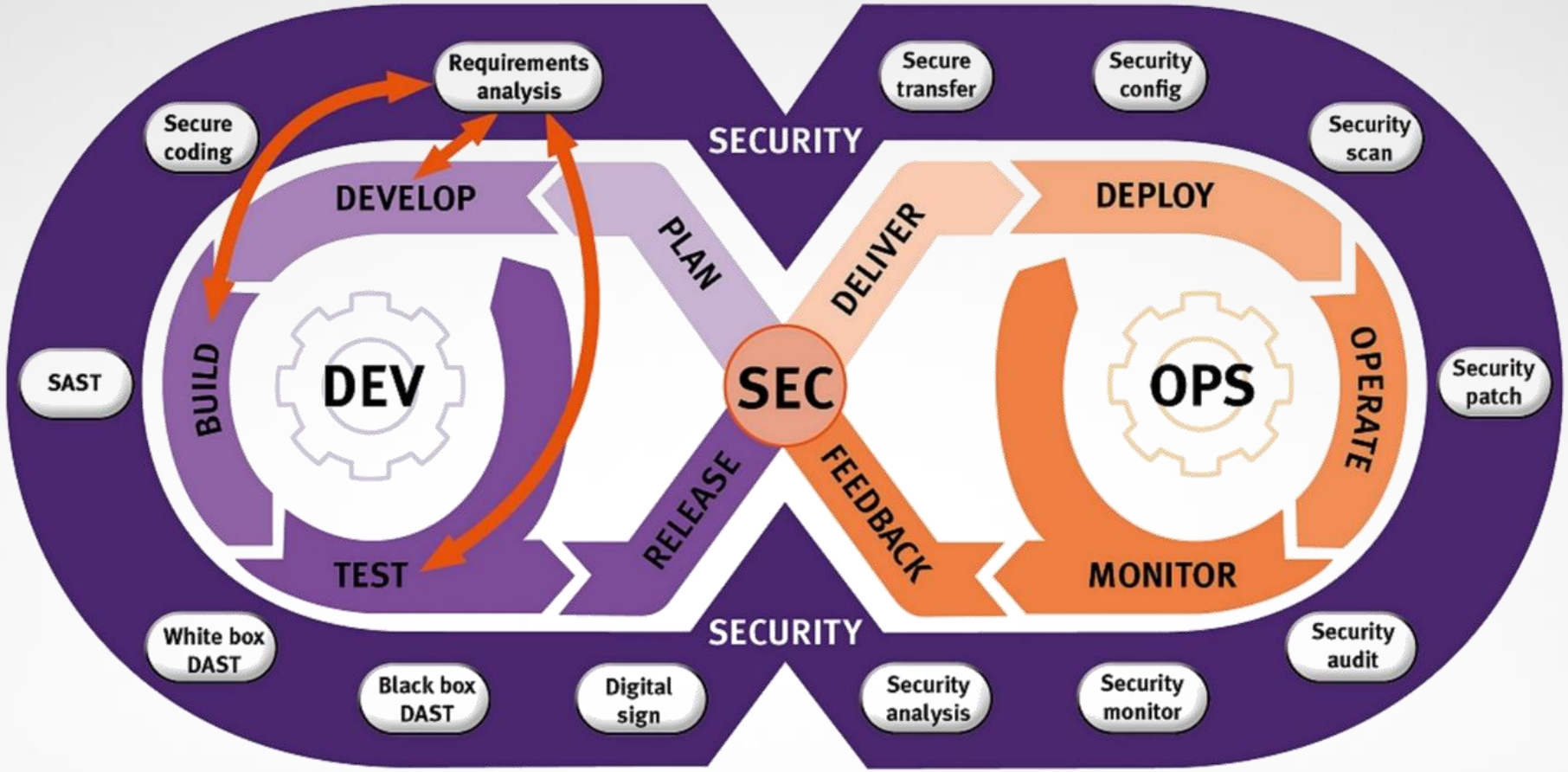


- 上线后发现漏洞风险更大、修复成本更高
- 能持续在软件上线前发现更多安全问题才能降低成本

火线

基于开源社区IAST的代码漏洞检测

DevSecOps应用安全工具链



SAST：白盒代码扫描

DAST：黑盒动态扫描

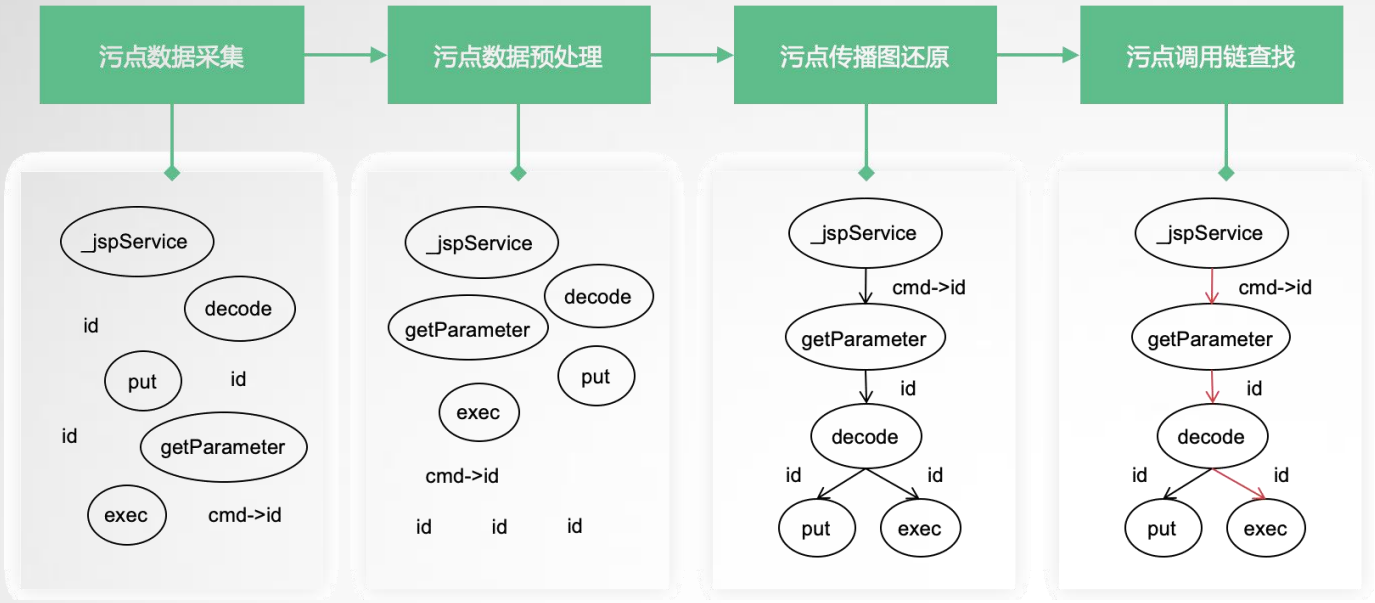
IAST：交互式动态污点分析

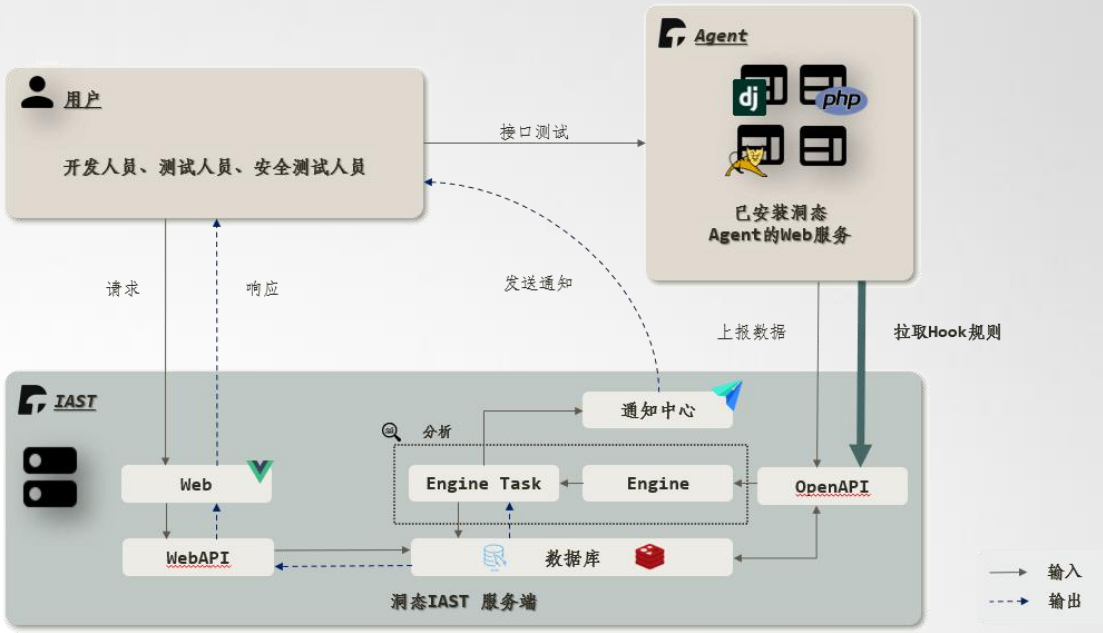
SCA：开源组件安全分析

DAST、SAST和IAST对比

对比项	DAST	SAST	IAST
可测试对象	Web 应用程序	Web 应用程序 App	Web 应用程序 App
漏洞检出率	中	高	高
漏洞误报率	低	高	极低（几乎为 0）
使用成本	较低	高（需人工排除误报）	低
脏数据	很多	较少	无
测试覆盖度	低	高	高
检测速度	随测试用例数量稳定增加	随代码量呈指数增加	实时监测
漏洞详情	详细程度一般， 只有请求	详细程度较高， 数据流+代码行数	详细程度高，请求+数据流+代码行数

独创的技术架构优势





- ✓低侵入式的数据采集端
- ✓高效零误报的技术优势
- ✓独特的应用数据仓储中心设计
- ✓具备可持续运营的产品设计
- ✓开放的社区生态持续贡献

IAST不同架构设计

Agent端检测

Agent端性能损耗高

无法构建统一的数据底座，数据无法得到充分的利用

新漏洞需重新下发规则重新扫描

无法进行微服务的调用链追踪

Server端检测

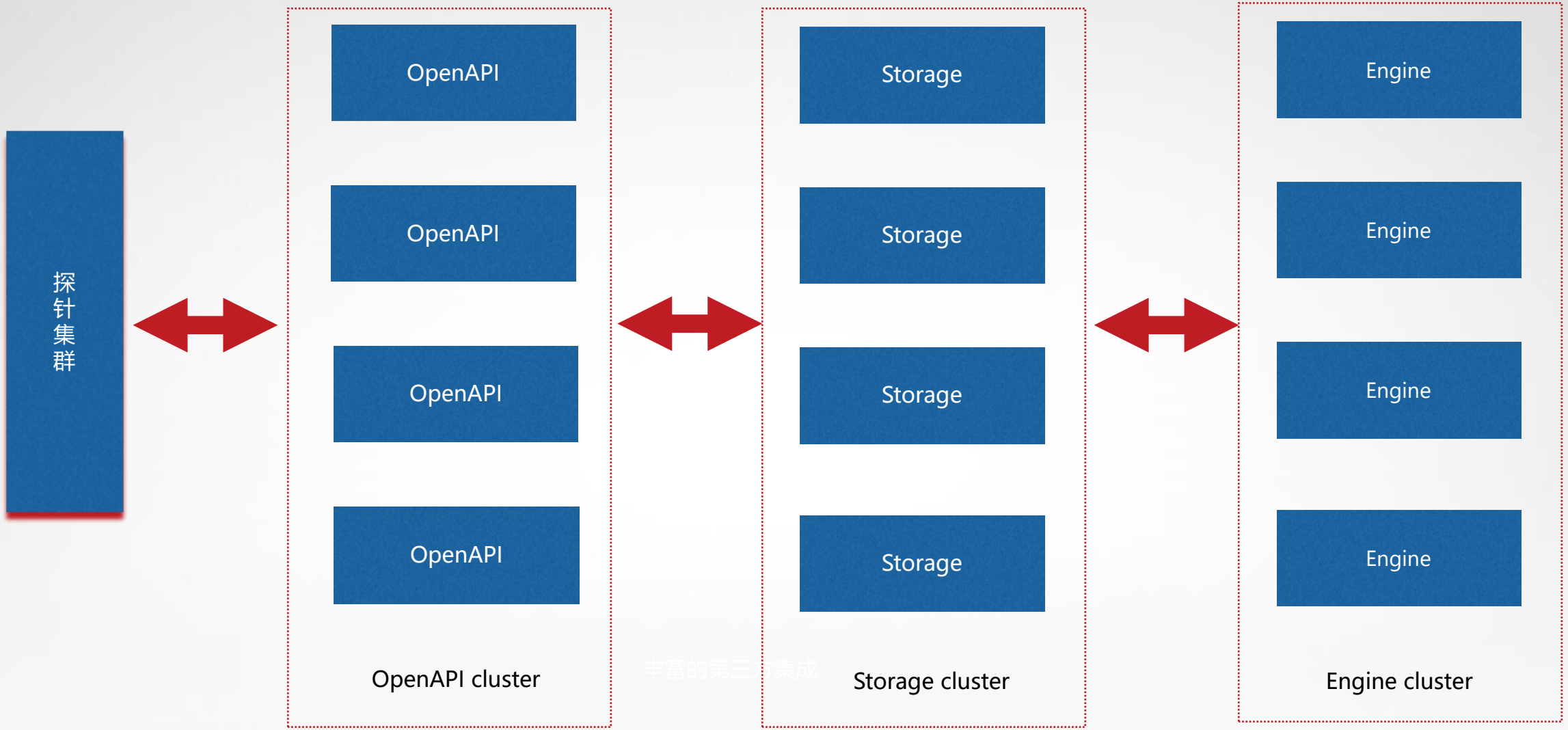
Agent端性能损耗高

构建统一的数据底座，数据得到充分的利用

新漏洞需重新下发规则重新扫描

无法进行微服务的调用链追踪

弹性扩容能力


探针集群
OpenAPI
OpenAPI
OpenAPI
OpenAPI
OpenAPI cluster
Storage
Storage
Storage
Storage
Storage cluster
Engine
Engine
Engine
Engine
Engine cluster

洞态IAST产品能力

1. 漏洞详情定位到代码行
2. 依赖组件的供应链风险排查
3. 梳理API Sitemap精准反馈未测试接口
4. 支持云原生的部署方式，一键启动
5. 统一探针上报的数据格式，利用数据分析实现漏洞的离线检测

组件梳理

maven:org.springframework.security:spring-security-core:5.2.1.RELEASE:

版本： 5.2.1.RELEASE

风险： 高危

项目： webgoat

漏洞数量： 2个

文件哈希： f1265ecdd4636a2038768c2ab9da4b79961a3465

漏洞列表

CVE 编号	CWE 编号	漏洞名称	漏洞等级	安全版本	操作
CVE-2020-5408	CWE-330	Information Disclosure	中危	5.2.4.RELEASE	
CVE-2020-5408	CWE-330	Information Disclosure	中危	5.2.4.RELEASE	

漏洞触发过程分析


IAST
项目配置
应用漏洞
组件管理
搜索
系统配置
组织管理
租户管理
部署IAST
请选择
1/367
刷新
/api/activity/m/h5-live/send...
低危
12分钟前
/api/activity/m/h5-live/heat.j...
低危
12分钟前
/api/c/v2/university/universit...
低危
50分钟前
/api/c/v2/live-activity/h5-liv...
低危
53分钟前
/api/c/v2/common/enum/qu...
低危
56分钟前
/api/c/v2/university/universit...
低危
56分钟前
/api/c/v2/person/person-list...
低危
56分钟前
/api/c/v2/common/country/li...
污点流图
污点来源
传播方法
危险方法
org/apache/catalina/connector/Request.getAttribute()
java.lang.StringBuilder.append()
java.lang.StringBuilder.toString()
java.lang.String.substring()
java.util.List.add()
java.util.List.toArray()
java.lang.StringBuilder.append()
类型
文件及行号
污点值
污点来源方法
org.apache.c... 282
2133098304
传播方法
org.springfra... 612
248838459
传播方法
org.springfra... 612
1006636517
传播方法
org.springfra... 1104
2041269256
传播方法
org.springfra... 1104
466184639
传播方法
org.springfra... 778
1173887485, ...
传播方法
org.springfra... 1154
1453648608

API Sitemap


洞态
项目配置
应用漏洞
组件管理
搜索
系统配置
组织管理
租户管理
+ Add Agent
springsec
JAVA
扫描模式 插桩模式
负责人 test002
最新时间 2021.08.24 12:37:44
版本
0824
报告导出
设置
项目概况
项目漏洞
项目组件
API导航
请选择请求方法
请选择覆盖状态
请输入API地址进行搜索
覆盖率 13.27%
GET
/vul/cmd-002
命令执行
参数列表
查看请求
名称
类型
额外信息
arg0
Map
GET请求参数
响应
String
GET
/vul/cmd-003/{cmd}

应用场景：更契合DevOps的漏洞检测产品

1. 低侵入式的技术方案
2. 高效零误报的技术优势

应用场景：安全能力沉淀

1. 安全能力沉淀传统安全工程师工作

   ➢手动/半自动安全测试、手动复测、安全运营

2. 基于IAST的安全工程师

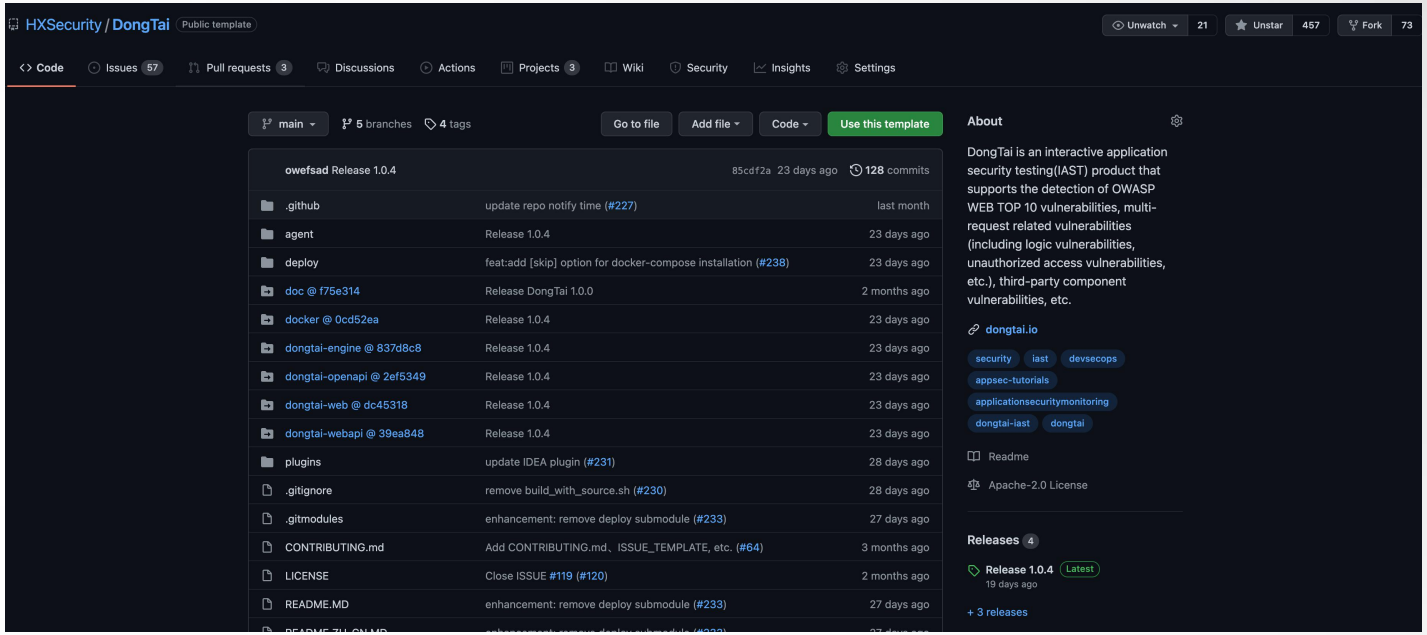
   ➢安全研究➔沉淀规则➔自动化漏洞检测➔自动通知➔自动复测

开源生态用户的落地支持

水滴筹　知乎

去哪儿旅行 总有你要的低价　轻松筹

等超过 100 家用户的真实落地



欢迎到展台详细交流

火线

THANKS

火 线 安 全

洞态

专注于网络安全行业，通过互联网平台、线下沙龙、培训、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流、学习的平台，培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。

官方网站:
https://www.anshijia.net.cn
微信公众号：asjeiss

安世加