巡风系统在同程运维安全的实践

刘新高

运维经理 同程旅游

北京 伦敦 纽约 旧金山 圣保罗 上海 | 东京

QCon
全球软件开发大会

[上海站]

信息安全
机器学习
人工智能
黑产
互联网金融（FinTech）
团队管理
基础设施
云计算
软件性能
硅谷
微服务
互联网架构

主办方 Geekbang. 极客邦科技 InfoQ

2017年10月17–19日
上海·宝华万豪酒店

扫描二维码
开启软件开发新思路

EGO聚变

TOGETHER CHANGE 2017

Geekbang 极客邦科技 | EGO EXTRA GEEKS' ORGANIZATION NETWORKS

EGO会员招募季

EGO旨在组建全球最具影响力的技术领导者社交网络，联结杰出的技术领导者学习和成长。

2017年6月30-7月10

扫码报名

SPEAKER

INTRODUCE

刘新高

- 开发多年，负责运维工作2年
- 运维系统设计与开发
- 喜欢C+Lua, 崇尚简单

目 录

CONCENTS

01 同程运维安全发展

02 巡风主机安全

03 巡风应用安全

04 巡风漏洞扫描

05 巡风开源

你的系统安全么？

SQL注入、XSS、越权

开发

网络边界、系统漏洞、应用配置不当

运维

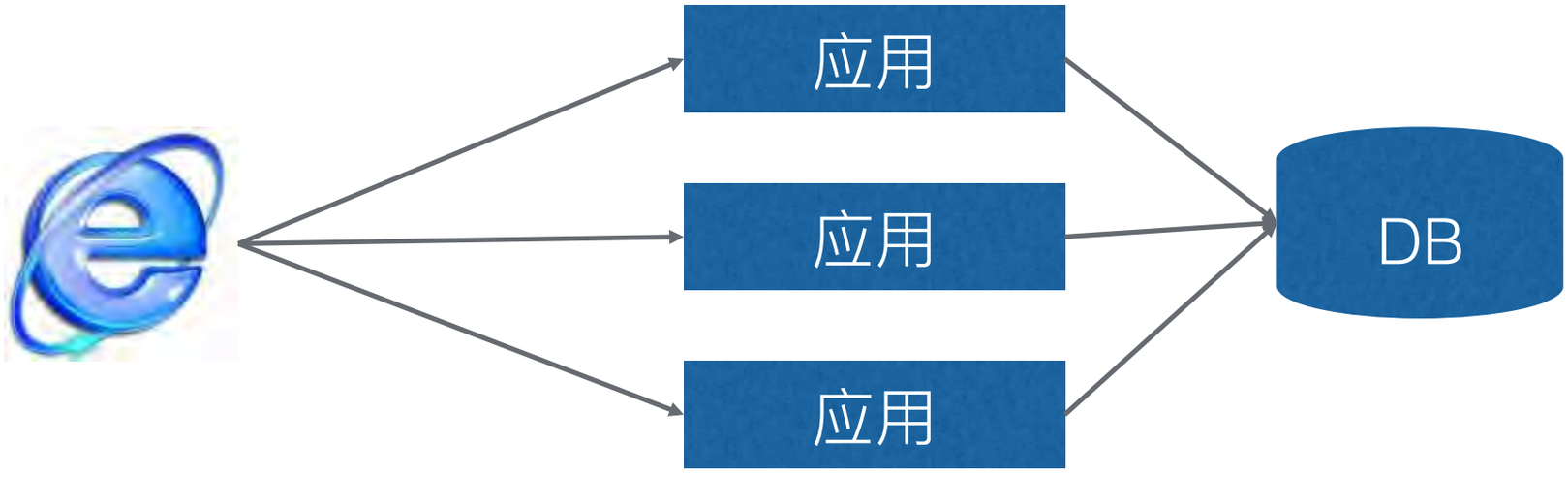
道高一尺，魔高一丈

同程运维安全初期

- 数十/数百台主机
- 应用简单
- 纯手工兼职运维
- 安全一般在开发的手上
- 没有防火墙，iptable/ipsec
- 服务器间没有隔离

- 不健壮密码/密码没有及时变更
- Web安全问题高发

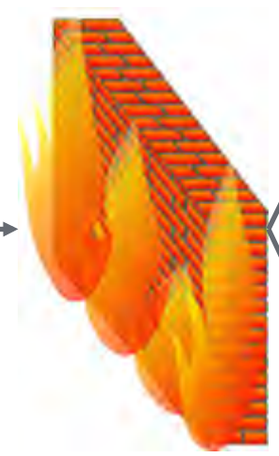
- 变更无记录、无法追溯
- 安全上没有规划、依赖少数人的人品

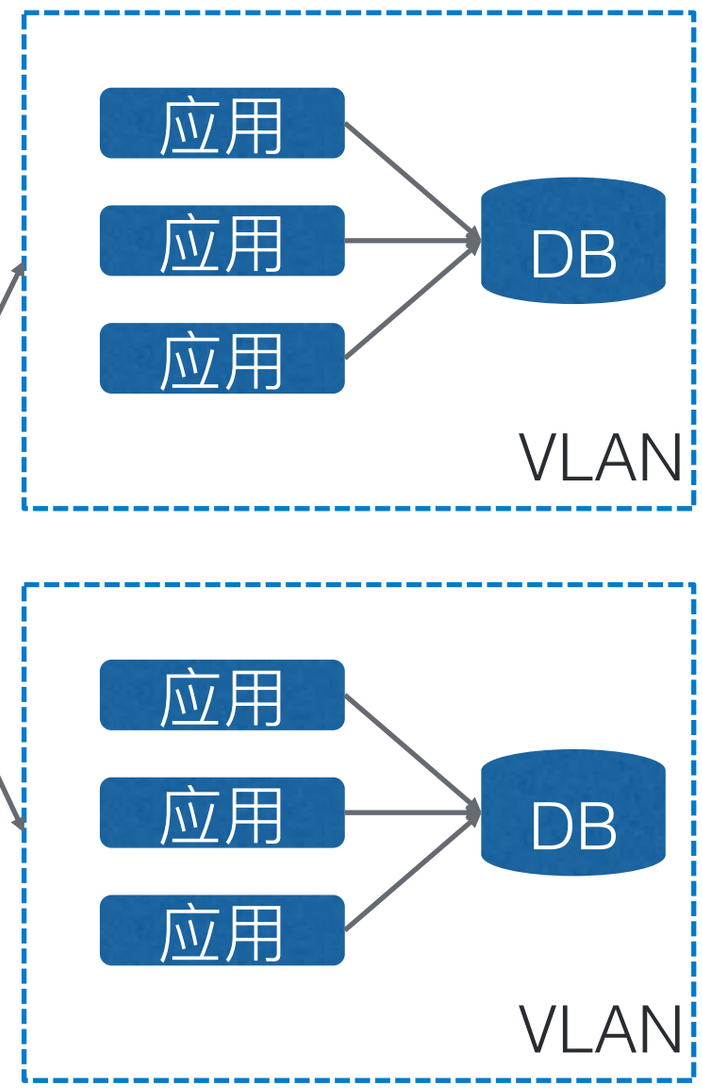


同程运维安全中期

- 数千台主机
- 有一定的自动化运维系统
- 划分不同的vlan
- 专业防火墙
- 有专门的运维人员及安全

- 特殊配置（成本、时间）
- 变更有一定记录
- 开放了不应该开放的服务

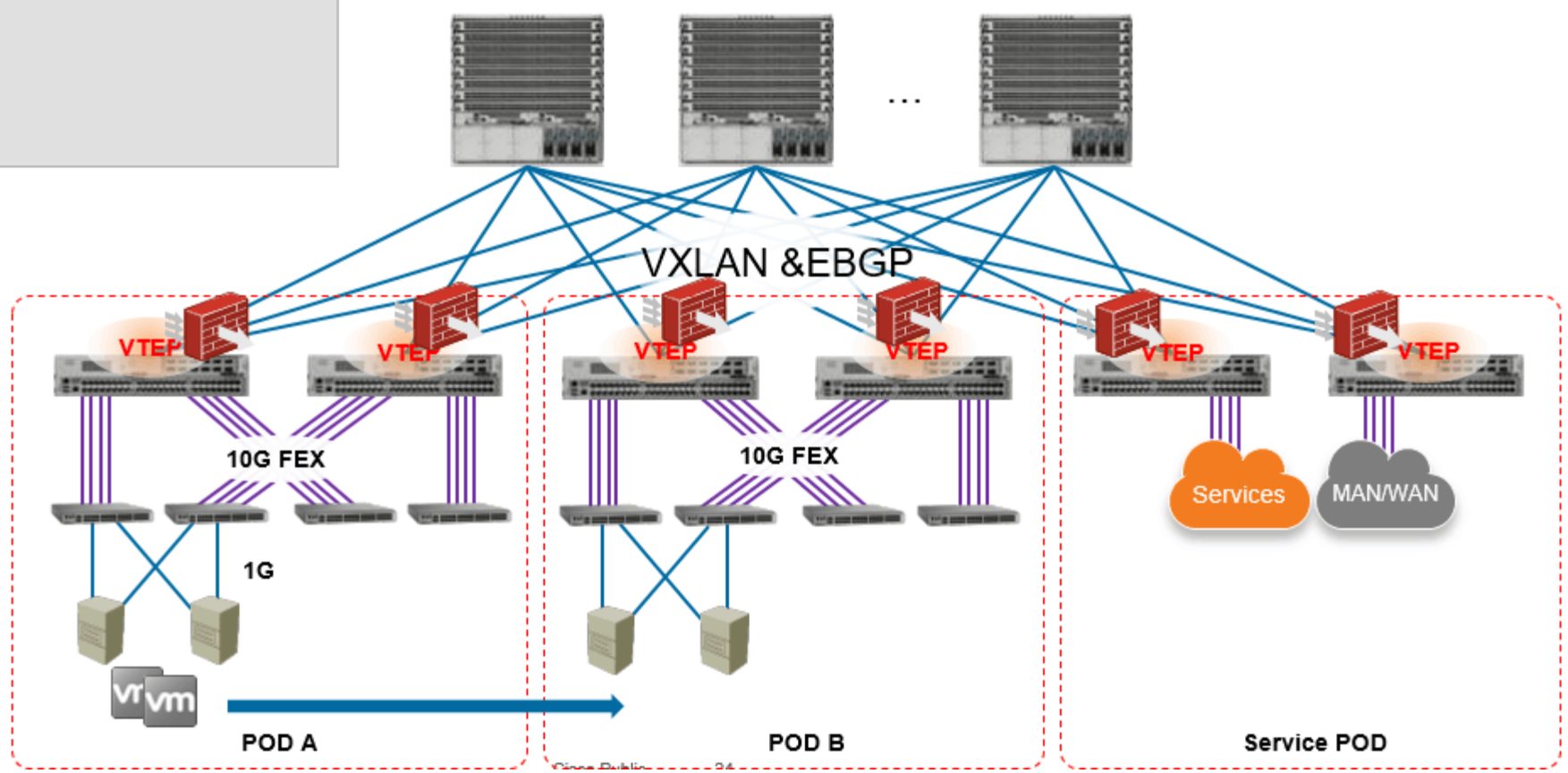




同程运维安全进行时

- 数万台实例
- 成熟自动化运维系统
- 专业的安全团队（YSRC）
- 安全系统

- 系统的复杂性
- 历史的包袱



运维与安全

系统漏洞

异常帐户

异常进程

未授权访问

异常端口

异常流量

违背最小化原则

异常连接

可疑文件

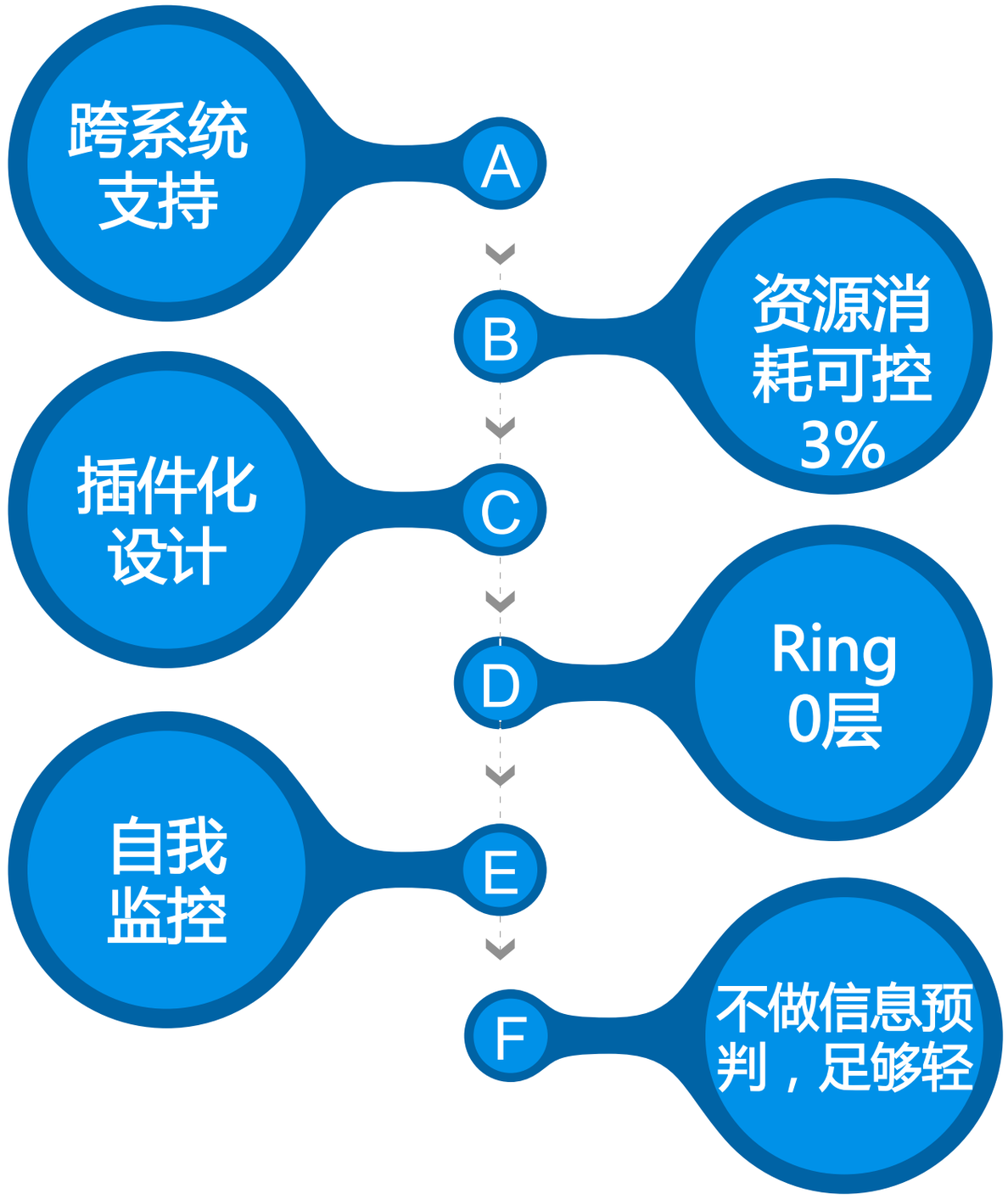
可写文件夹执行

应用配置不当

自动化运维能解决以上问题么？

巡风主机安全

巡风主机安全Agent—设计

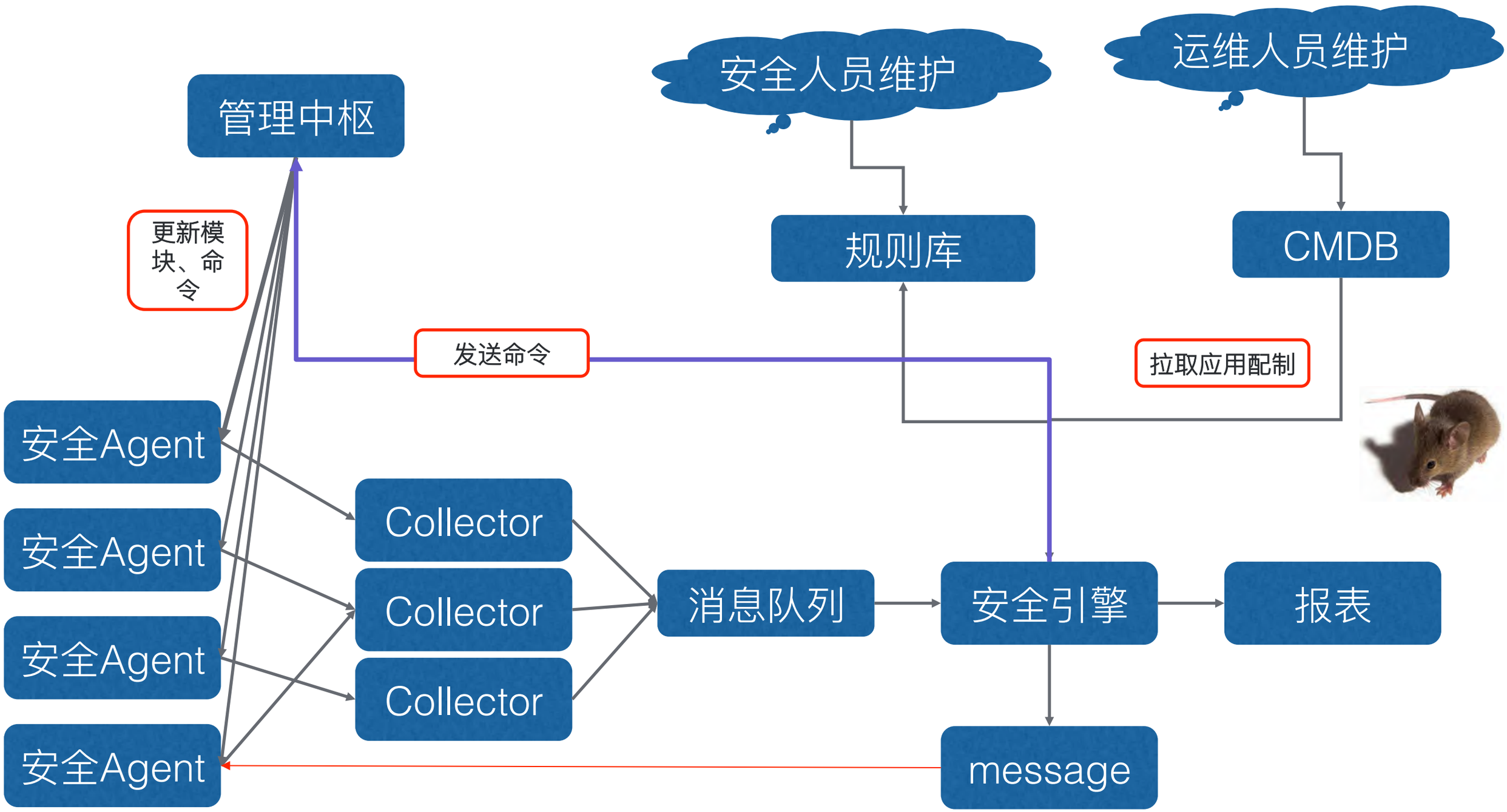


巡风主机安全Agent—功能

- WebShell检测（支持ASPX、PHP、Jsp）
- 异常网络行为检测
- 进程/命令监控
- 文件操作监控
- 安全基线核查
- 安全事件阻断

- 系统日志收集
- 系统信息（开机启动、服务列表、计划任务、开放端口、用户列表）收集
- 执行任务推送
- 漏洞补丁升级

巡风主机安全Agent-架构

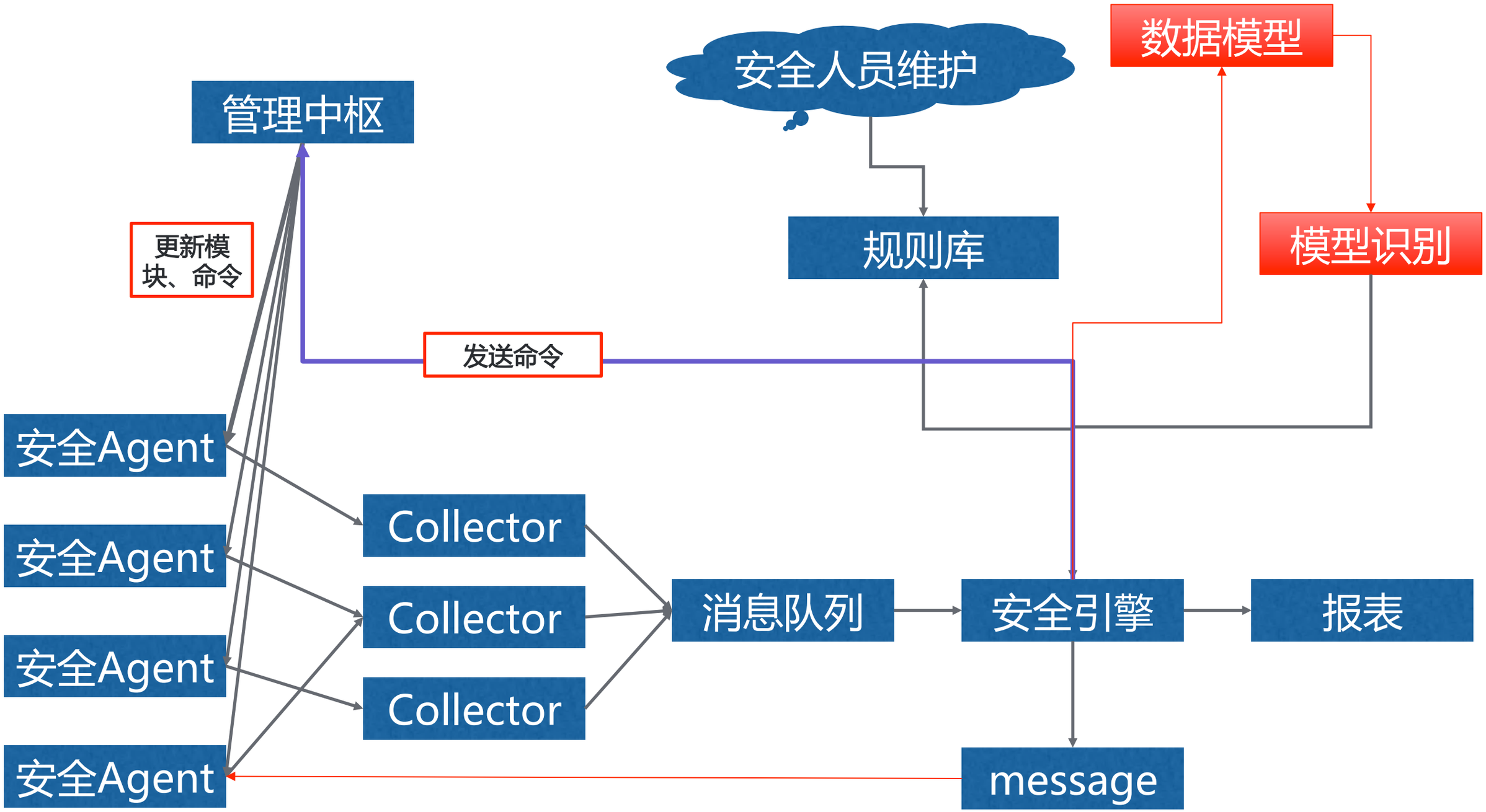


巡风主机安全Agent-数据驱动

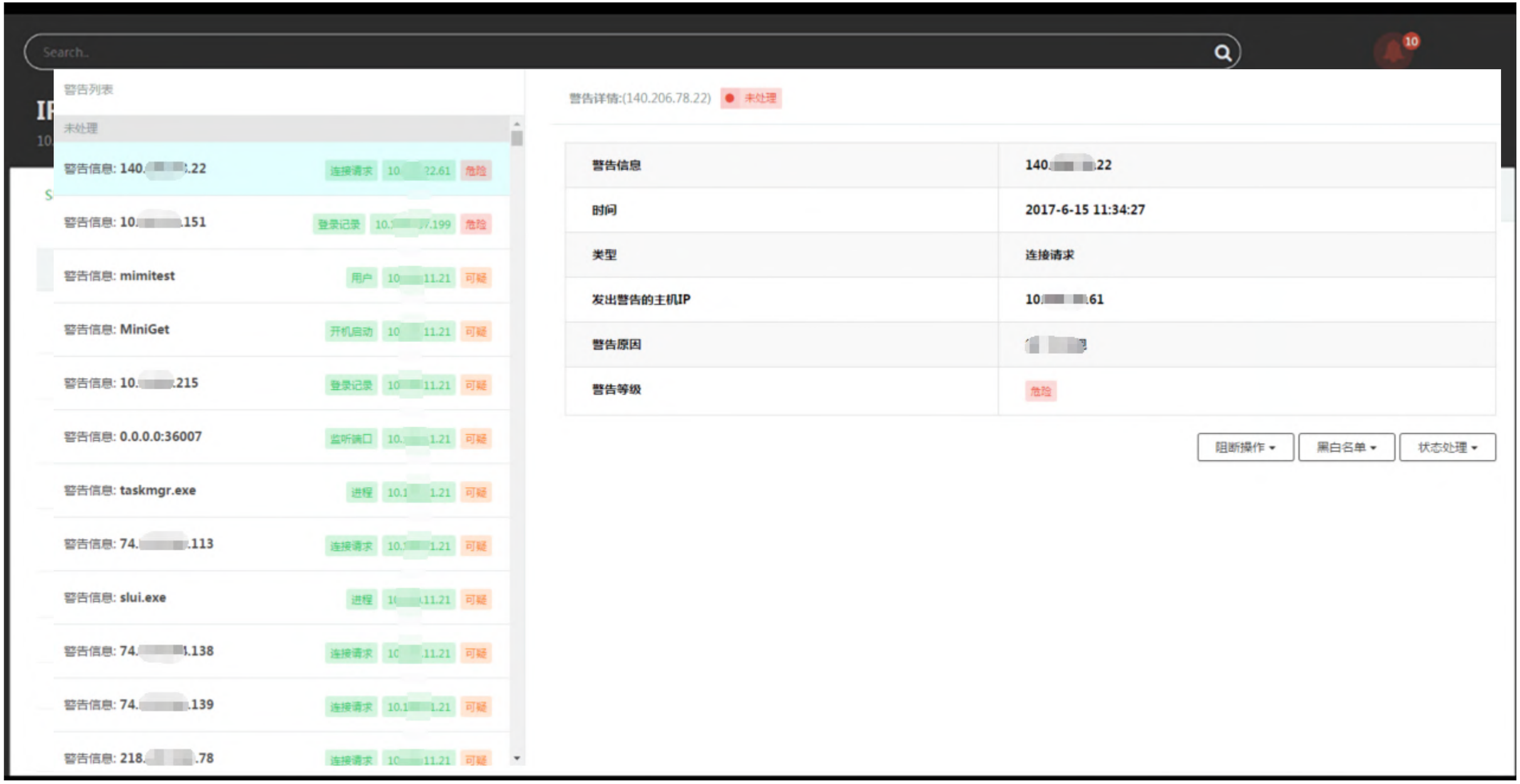
各种规则，配的累么？

新上一个服务，能整的清楚么？

巡风主机安全Agent-数据驱动



巡风主机安全Agent

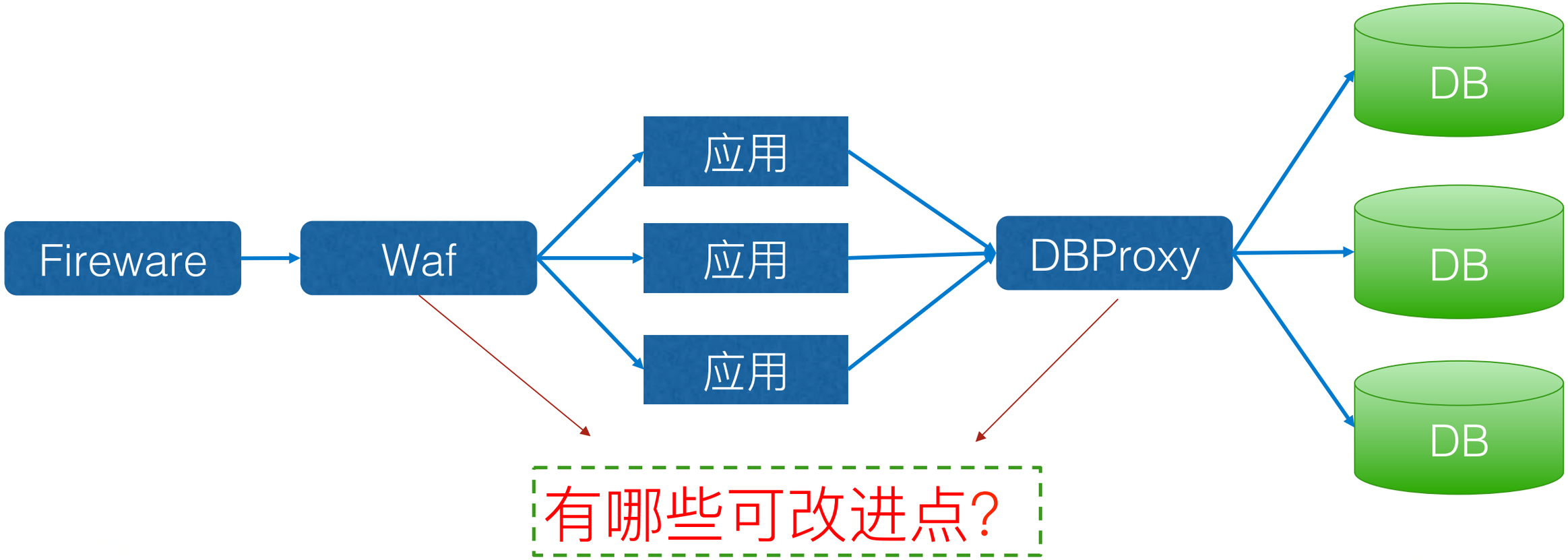


目前安全主机Agent产线已全覆盖，每天收集的信息量在千万量级，其中人工干预约半个工作日。

巡风应用安全模块

应用安全——传统设计

SQL注入
XSS攻击
越权问题?
Web Shell

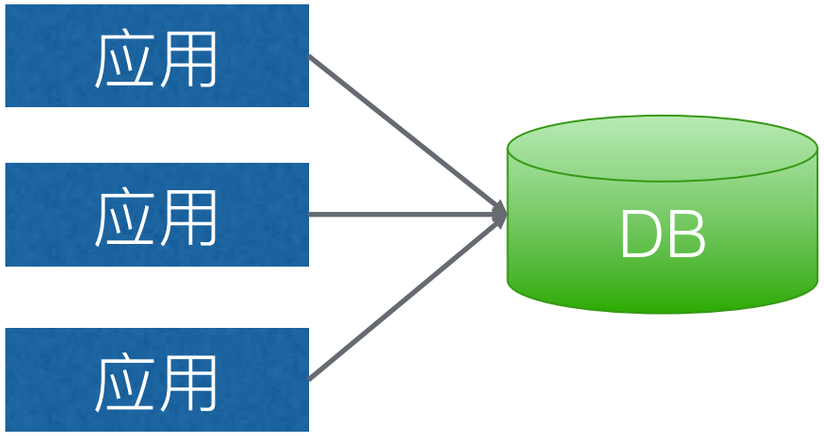


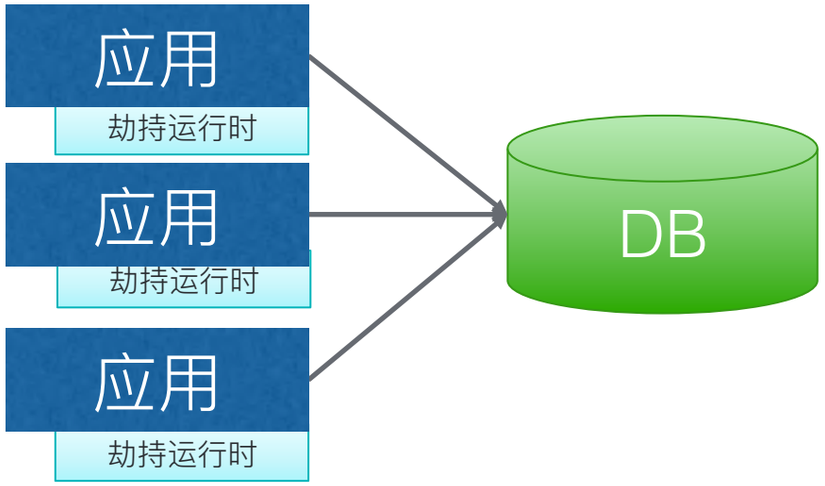
巡风应用安全模块

异常SQL
异常请求
异常访问

实时分析

预警/阻断





巡风应用安全模块

劫持关键方法点

- WebHandler.DoRequest
- HttpClient.Post()
- HttpClient.Get()
- SqlCommand.Excute()

- Socket.Create()
- File.Create

获取

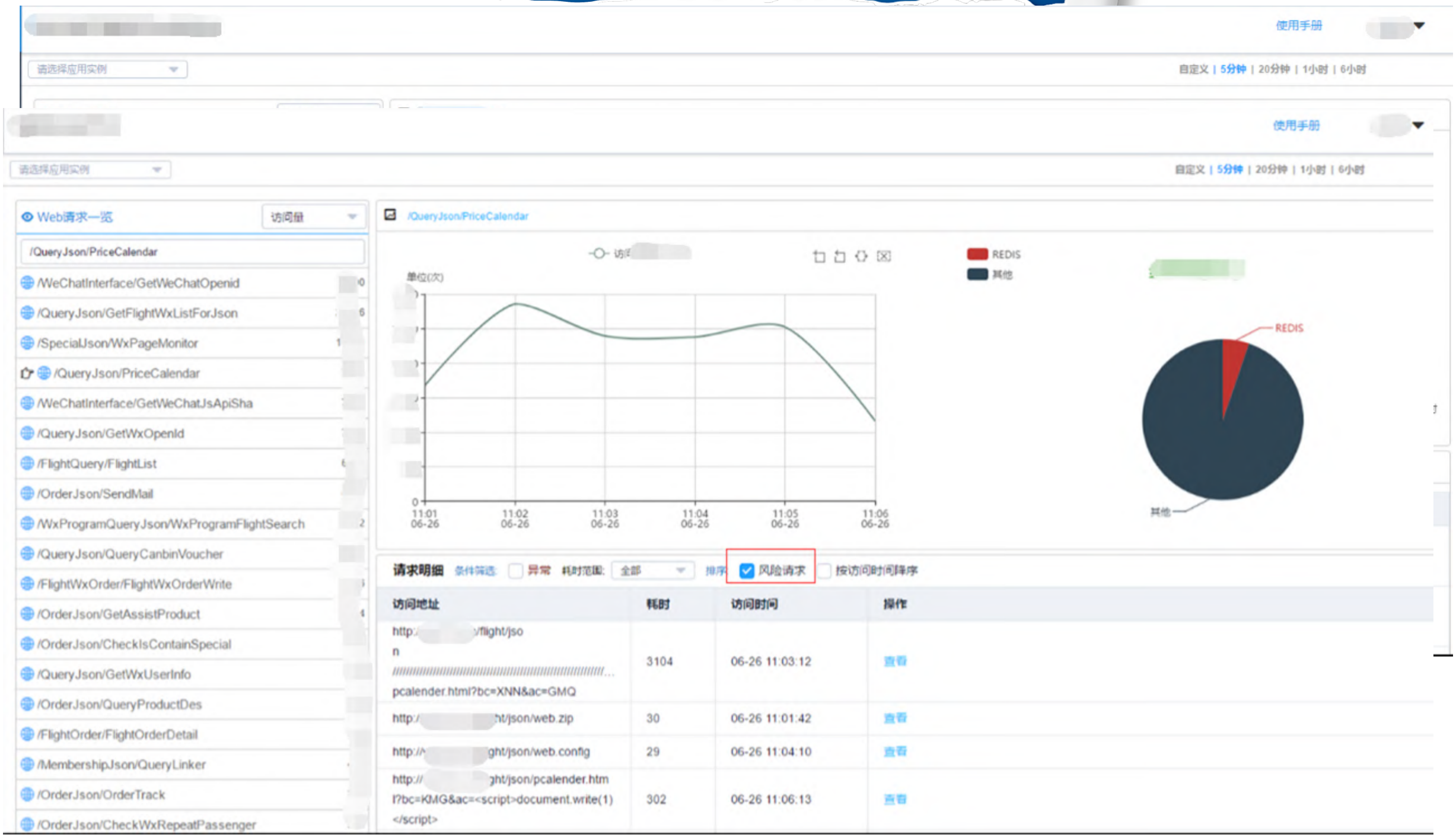
- ✓ Url+Para
- ✓ Url +Para
- ✓ Sql+Database

- ✓ IP+Port
- ✓ FileName

对于异常SQL、请求可以进行实时阻断。

目前每天处理百亿量级的数据，异常在百万级

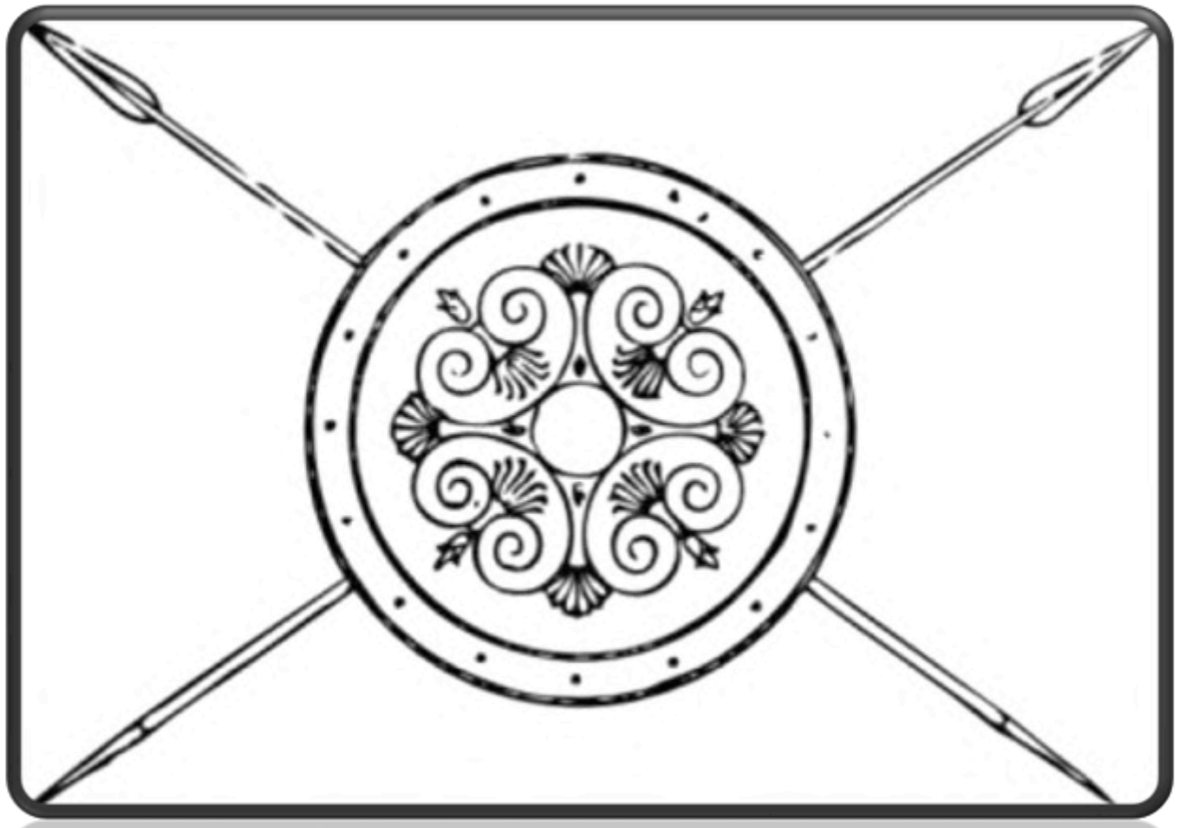
巡风应用安全模块



使用手册
请选择应用实例
自定义 | 5分钟 | 20分钟 | 1小时 | 6小时
Web请求一览
访问量
/QueryJson/PriceCalendar
/WeChatInterface/GetWeChatOpenid
/QueryJson/GetFlightWxListForJson
/SpecialJson/WxPageMonitor
/QueryJson/PriceCalendar
/WeChatInterface/GetWeChatJsApiSha
/QueryJson/GetWxOpenId
/FlightQuery/FlightList
/OrderJson/SendMail
/WxProgramQueryJson/WxProgramFlightSearch
/QueryJson/QueryCanbinVoucher
/FlightWxOrder/FlightWxOrderWrite
/OrderJson/GetAssistProduct
/OrderJson/CheckIsContainSpecial
/QueryJson/GetWxUserInfo
/OrderJson/QueryProductDes
/FlightOrder/FlightOrderDetail
/MembershipJson/QueryLinker
/OrderJson/OrderTrack
/OrderJson/CheckWxRepeatPassenger
REDIS
其他
单位(次)
11:01 06-26
11:02 06-26
11:03 06-26
11:04 06-26
11:05 06-26
11:06 06-26
请求明细
条件筛选:
异常
耗时范围:
全部
排序
风险请求
按访问时间降序
访问地址
耗时
访问时间
操作
3104
06-26 11:03:12
查看
30
06-26 11:01:42
查看
29
06-26 11:04:10
查看
302
06-26 11:06:13
查看

巡风漏洞扫描模块

巡风漏洞扫描模块



目前巡风扫描模块漏洞检测插件150+
每天扫描任务量级在数十万以上

巡风漏洞扫描模块

网络资产识别：

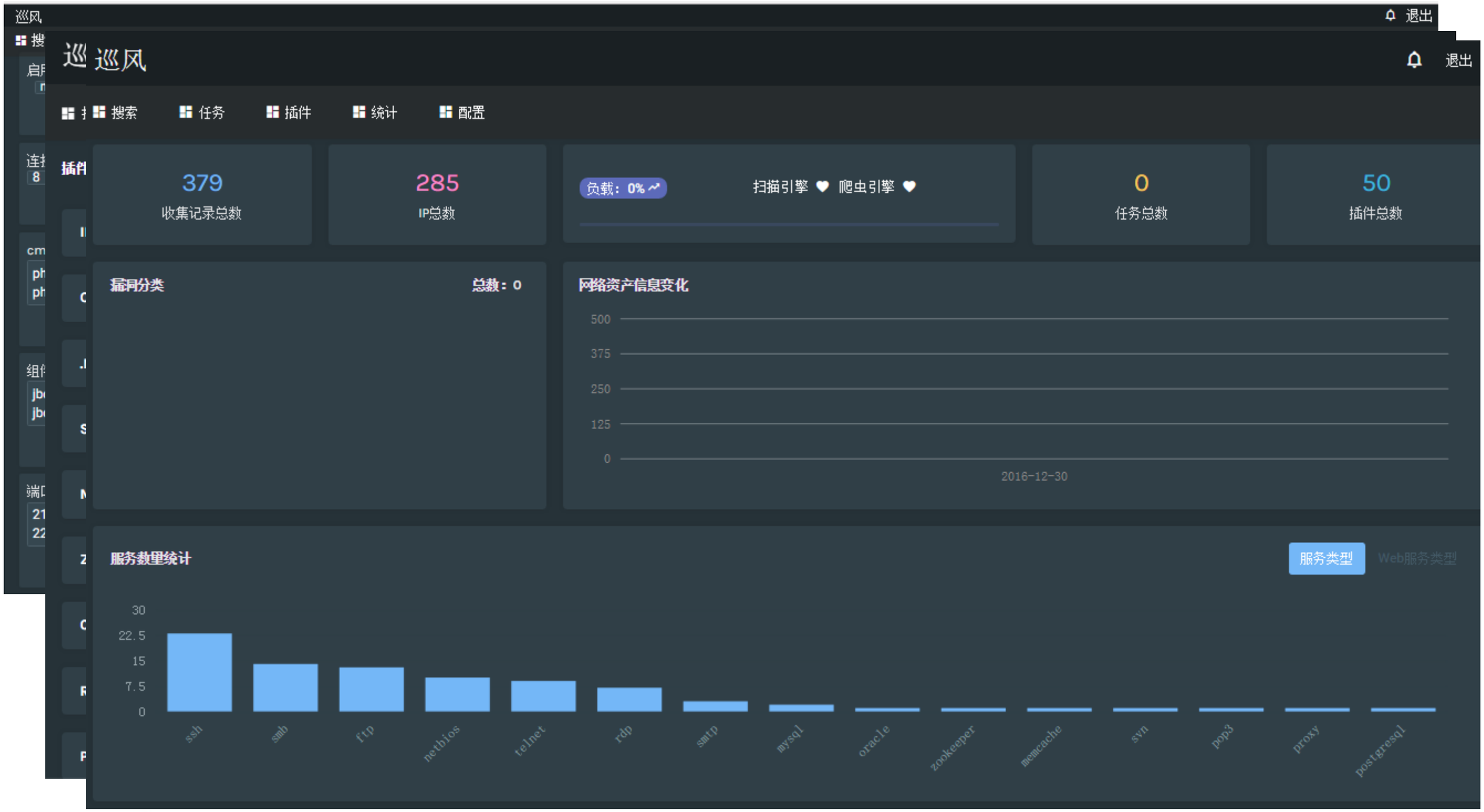
端口探测
指纹识别（服务类型、组件容器、脚本语言）

漏洞检测引擎:

定期或者一次性的漏洞检测
2种插件类型、标识符与脚本
巡风主机agent主动触发

同程安全开源 ——《巡风系统》

github地址如下：https://github.com/ysrc/xunfeng



同程巡风系统——NEXT

- 应用安全模块支持更多语言、数据库
- 主机安全模块，多环境策略支持
- 各模块风险策略统一分级、评分
- 与业界共享安全信息、进一步开源

THANKS!

让创新技术推动社会进步

HELP TO BUILD A BETTER SOCIETY WITH
INNOVATIVE TECHNOLOGIES

Geekbang.
极客邦科技

InfoQ

专注中高端技术人员的技术媒体

EGO EXTRA GEEKS' ORGANIZATION NETWORKS

高端技术人员学习型社交平台

StuQ 斯达克学院

实践驱动的 IT 教育平台

地址：北京市朝阳区洛娃大厦C座8层1801室　　网址：www.geekbang.org