网藤黑科技揭秘

架构师 王珉然（wofeiwo）

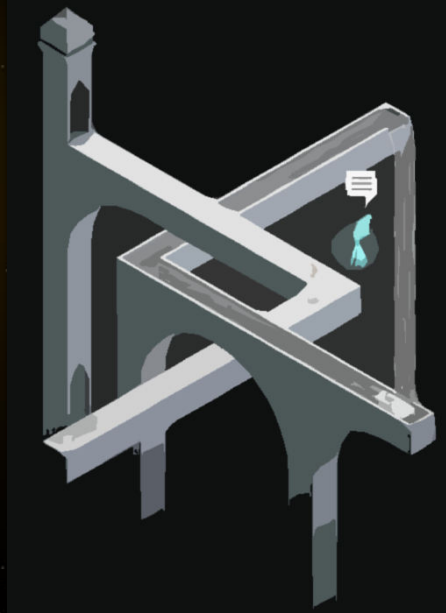
目标

安全的感知

资产、数据、安全联动

企业化安全服务


资产识别
拓扑建模
安全扫描
结果汇总
修复流程
回归测试
持续监测



一片混沌

关键资产识别

任务顺序依赖处理

各类型扫描调度

成百资产

成千扫描插件

实时结果反馈

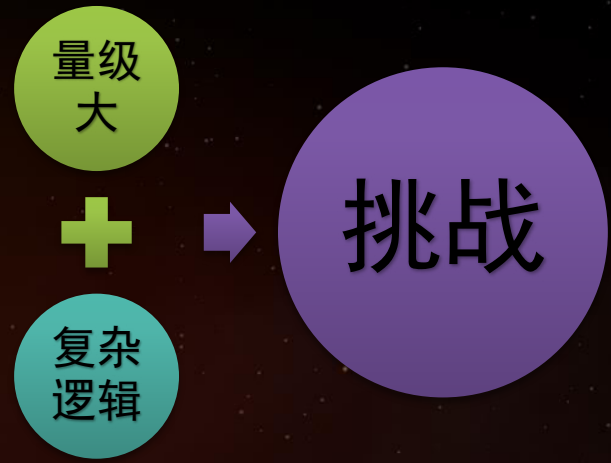
1 task = 10000 Job

1000 task = ?? job

“任何一事物，在数量巨大的情况下，就会产生质变。”

“任何一事物，当关联复杂的时候，难度就几何级数增长。”

挑战大

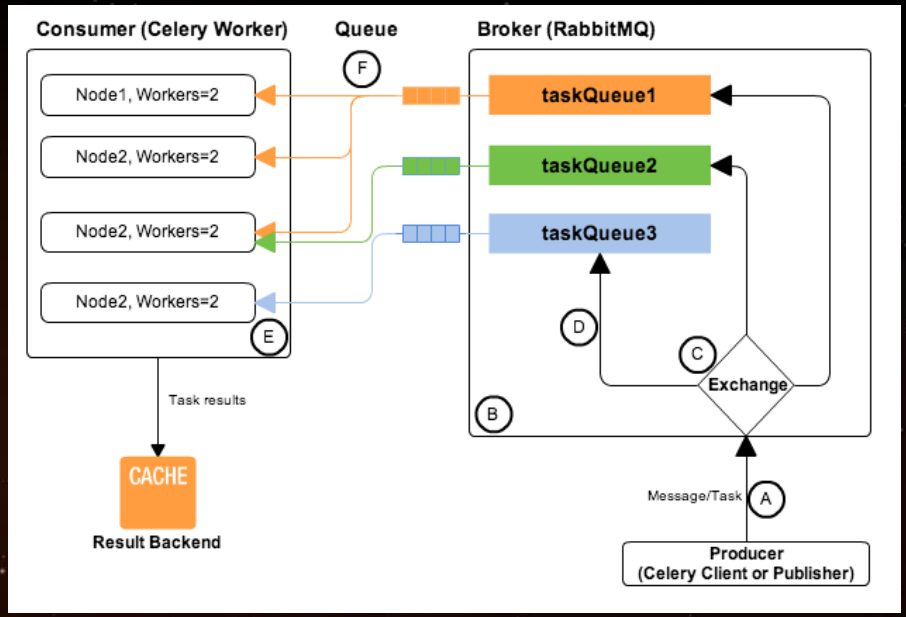


网藤怎么实现？

三种武器

分布式基础架构

Celery + RabbitMQ



灵活的任务调度

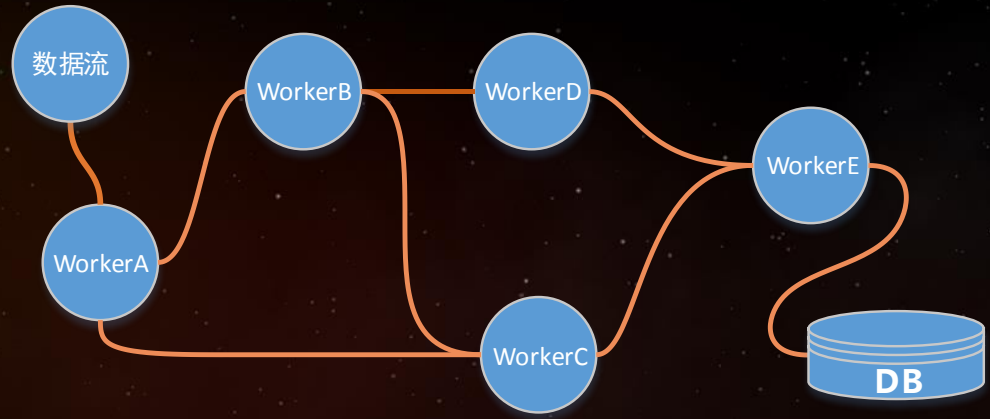
- 20000+任务
- 毫秒级任务下发
- 错误自动化恢复

可伸缩多节点

- 36节点（6国外节点）
- 3队列备份

流式任务处理

协程+异步大并发 I/O



巨量检测插件

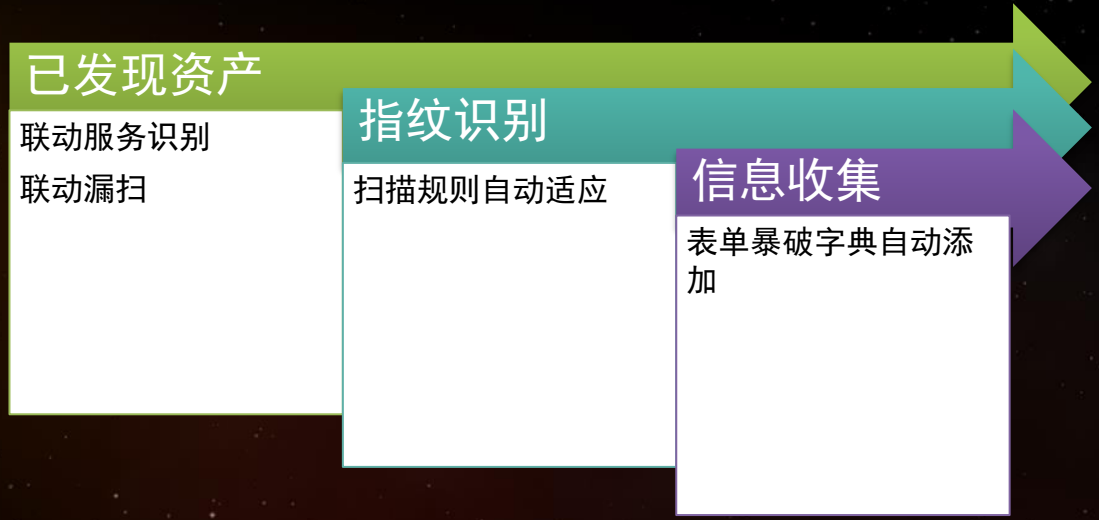
- 6种不同的资产探识方案
- 1000+检测模型
- 多种复杂策略集组合

高效率的检测性能

- 2000 req/s

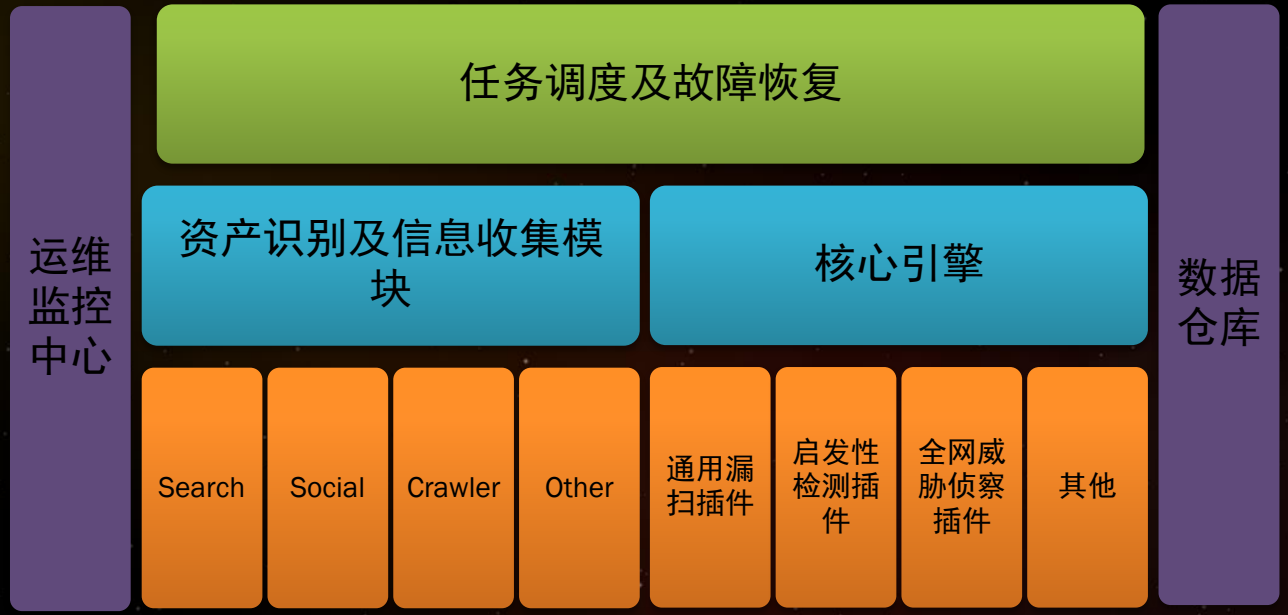
资产与数据联动

启发式漏洞感知



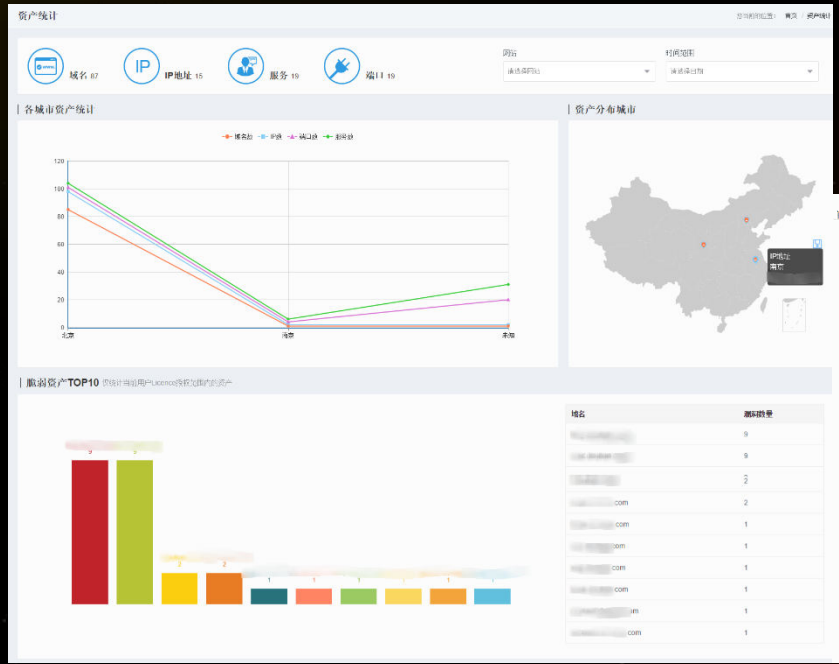
更少安全死角

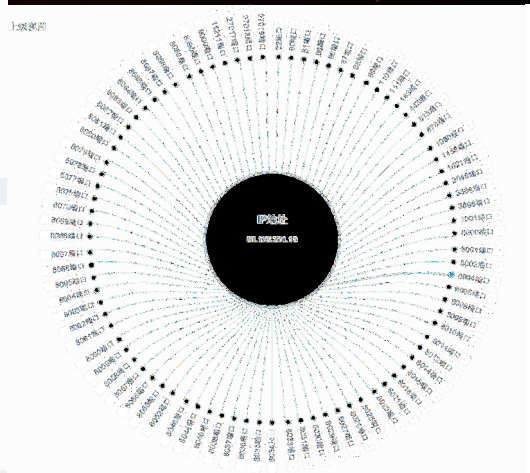
持续性的感知

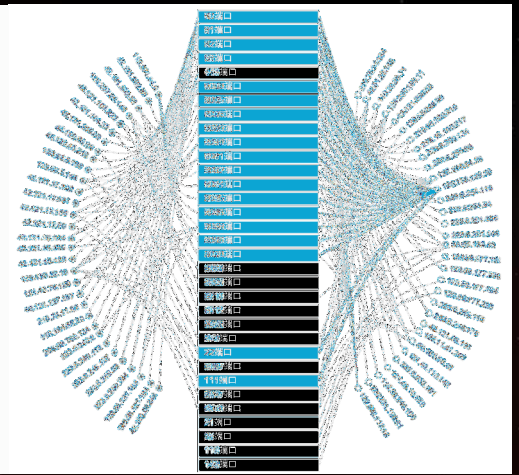

运维监控中心
任务调度及故障恢复
资产识别及信息收集模块
核心引擎
数据仓库
Search
Social
Crawler
Other
通用漏扫插件
启发性检测插件
全网威胁侦察插件
其他

产品

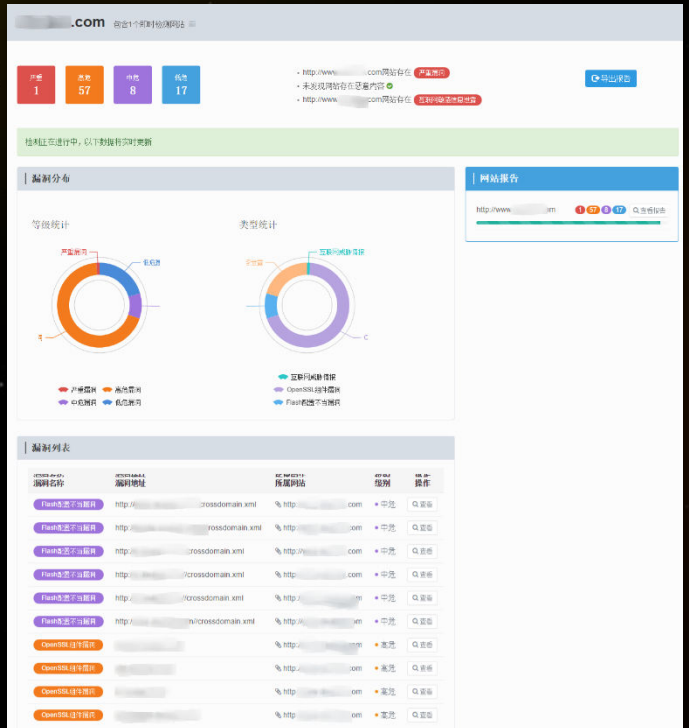
数据可视化　一目了然







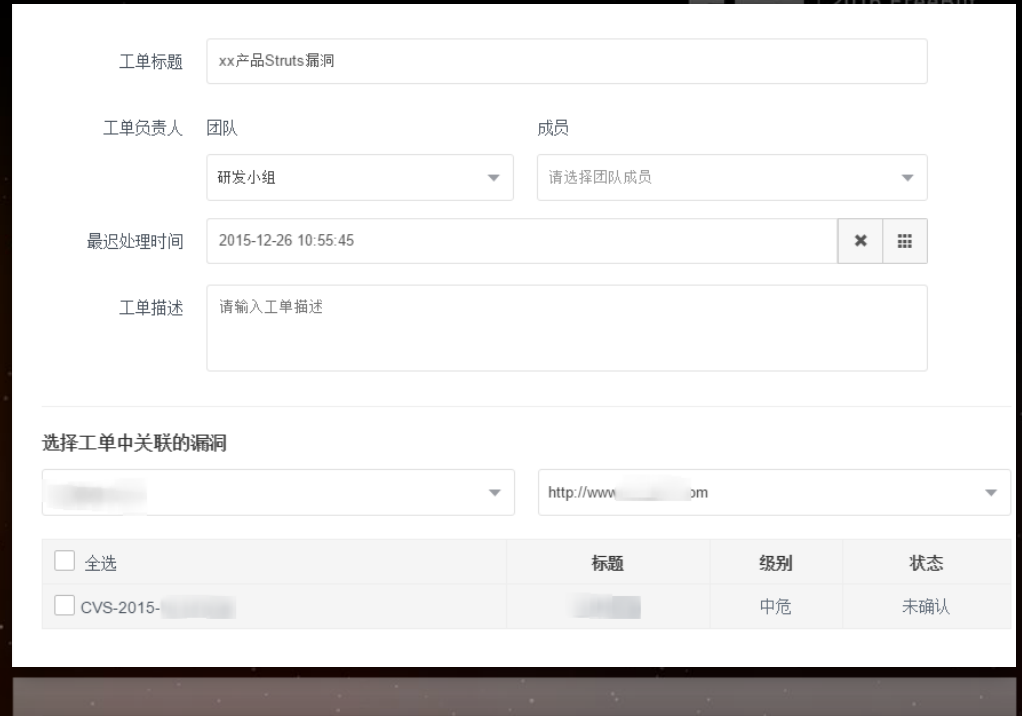
实时结果查看



当前状态	危险等级	创建时间	操作
95%	1 57 8 17	2015-12-29 16:31:06	实时结果

漏洞自动跟踪

自动化回归测试



特点	传统扫描器	网藤
部署方式	客户端设备	无需部署
隐藏资产发现	X	√
资产威胁建模联动	X	√
启发式检测	X	√
持续性监测	X	√
漏洞生命周期管理	X	√
实时结果	部分	√
在线专家支持	X	√

谢谢

https://cvs.vulbox.com