2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

多维安全漏洞治理

提升数据信息资产安全

东方证券 邬晓磊

目录

1 管理痛点

安全趋势的变化

边界安全

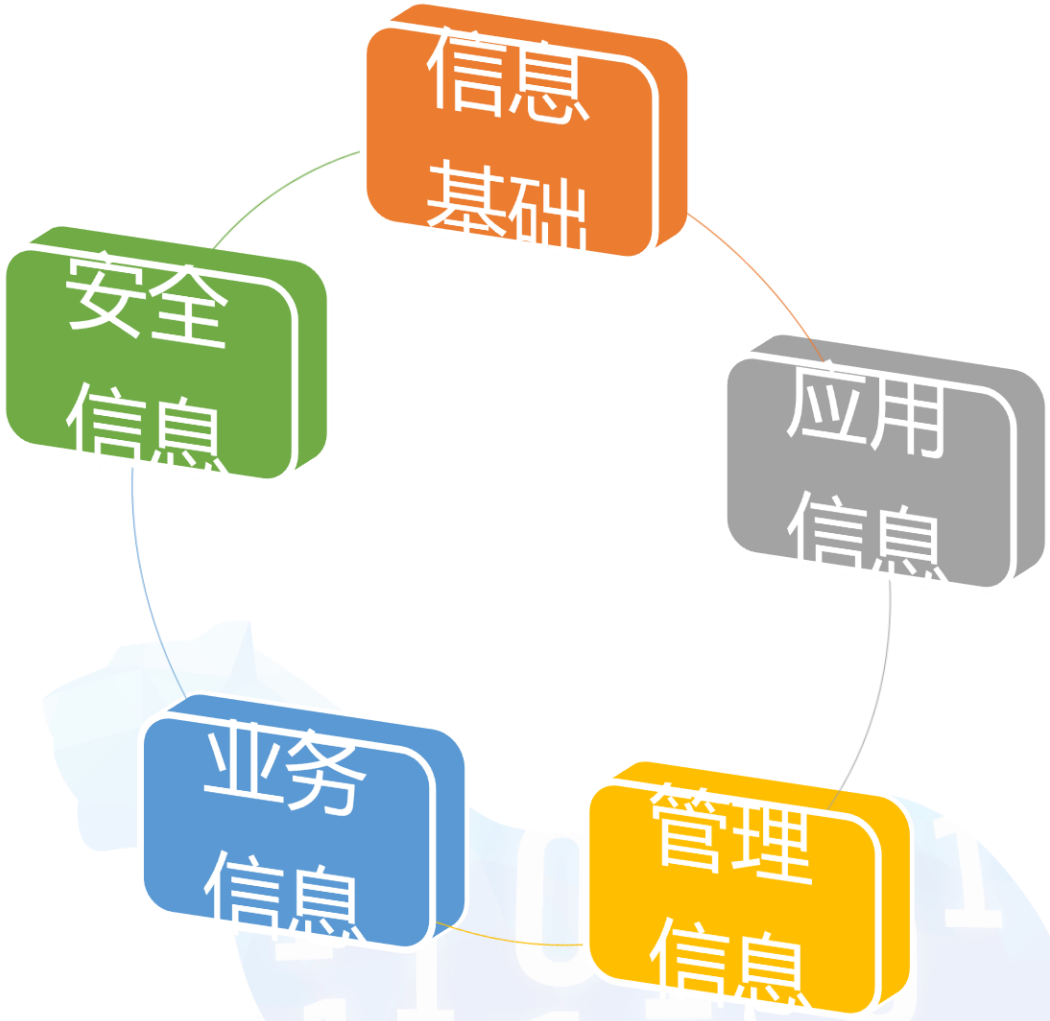
纵深安全

外挂式安全

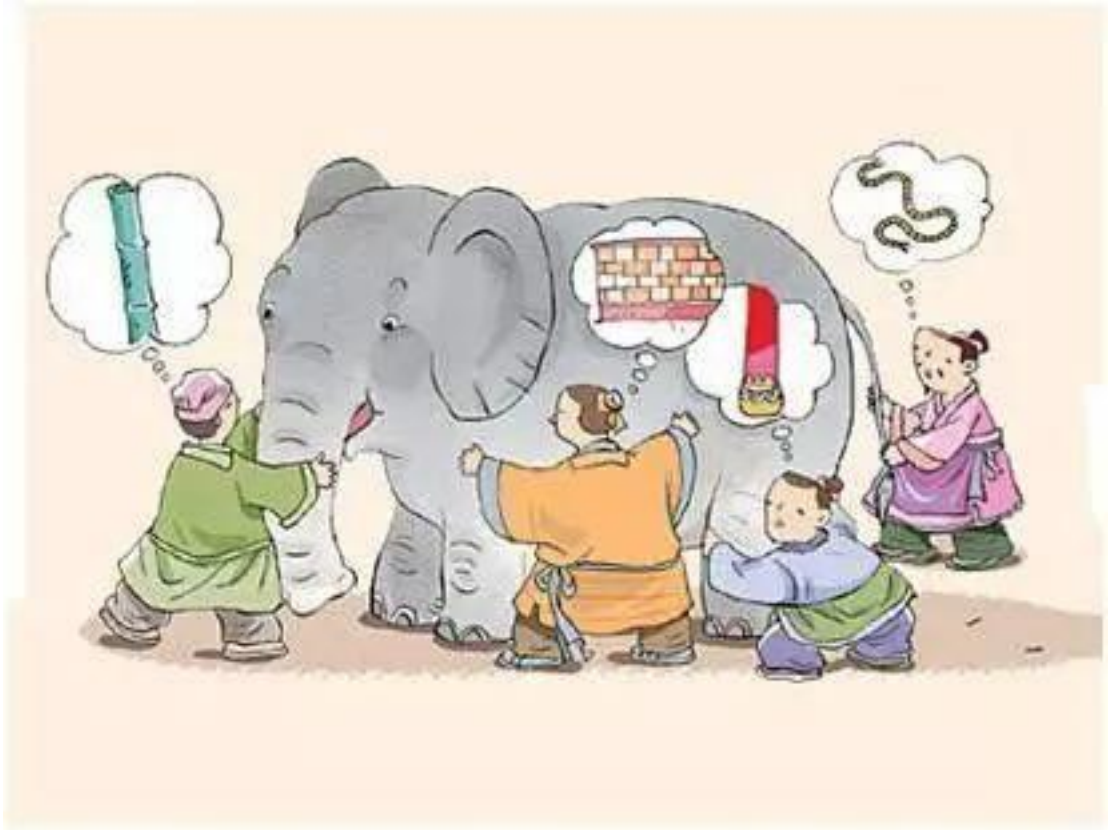
原生安全

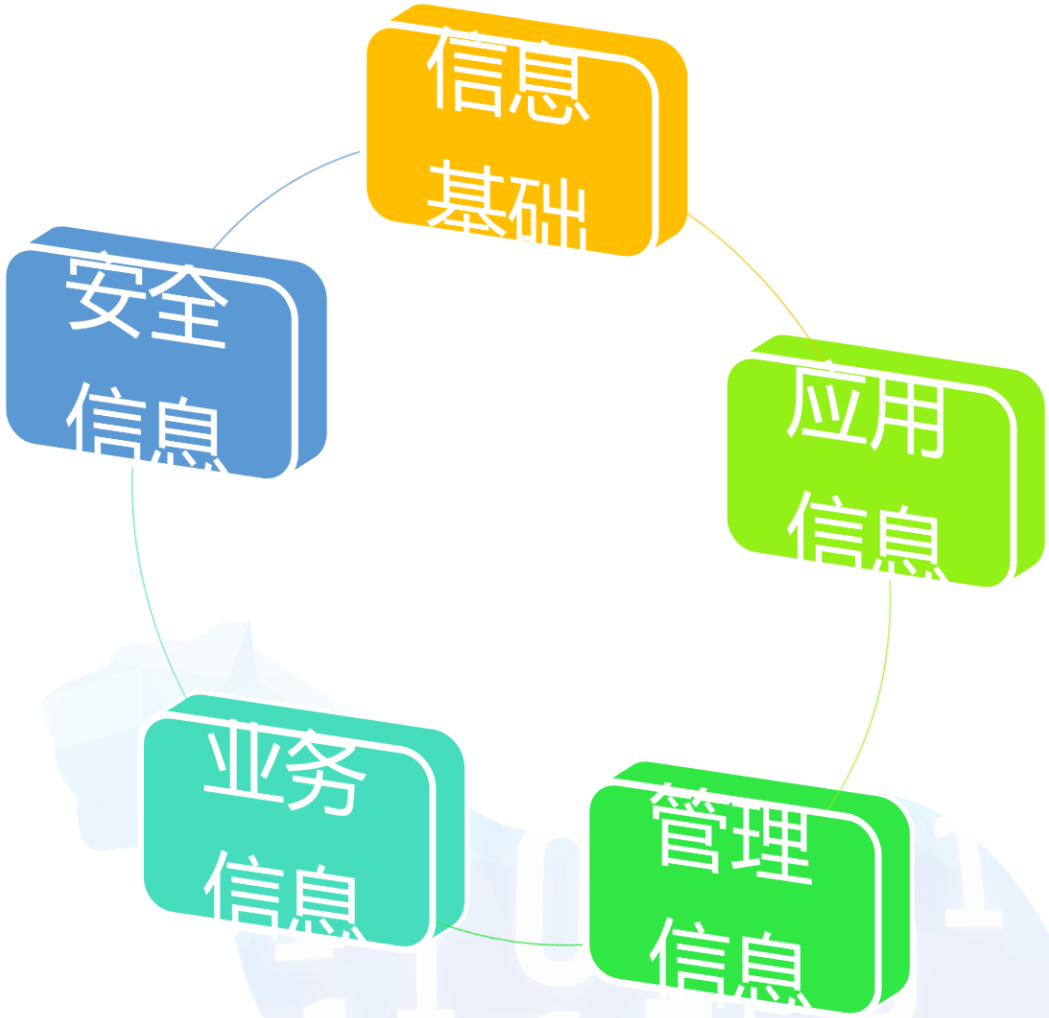
资产威胁管理的痛点

- 信息维度多
- 数据种类多
- 数据依赖人工处理
- 数据关联度不高



资产威胁管理的痛点





解决思路

高价值的CMDB

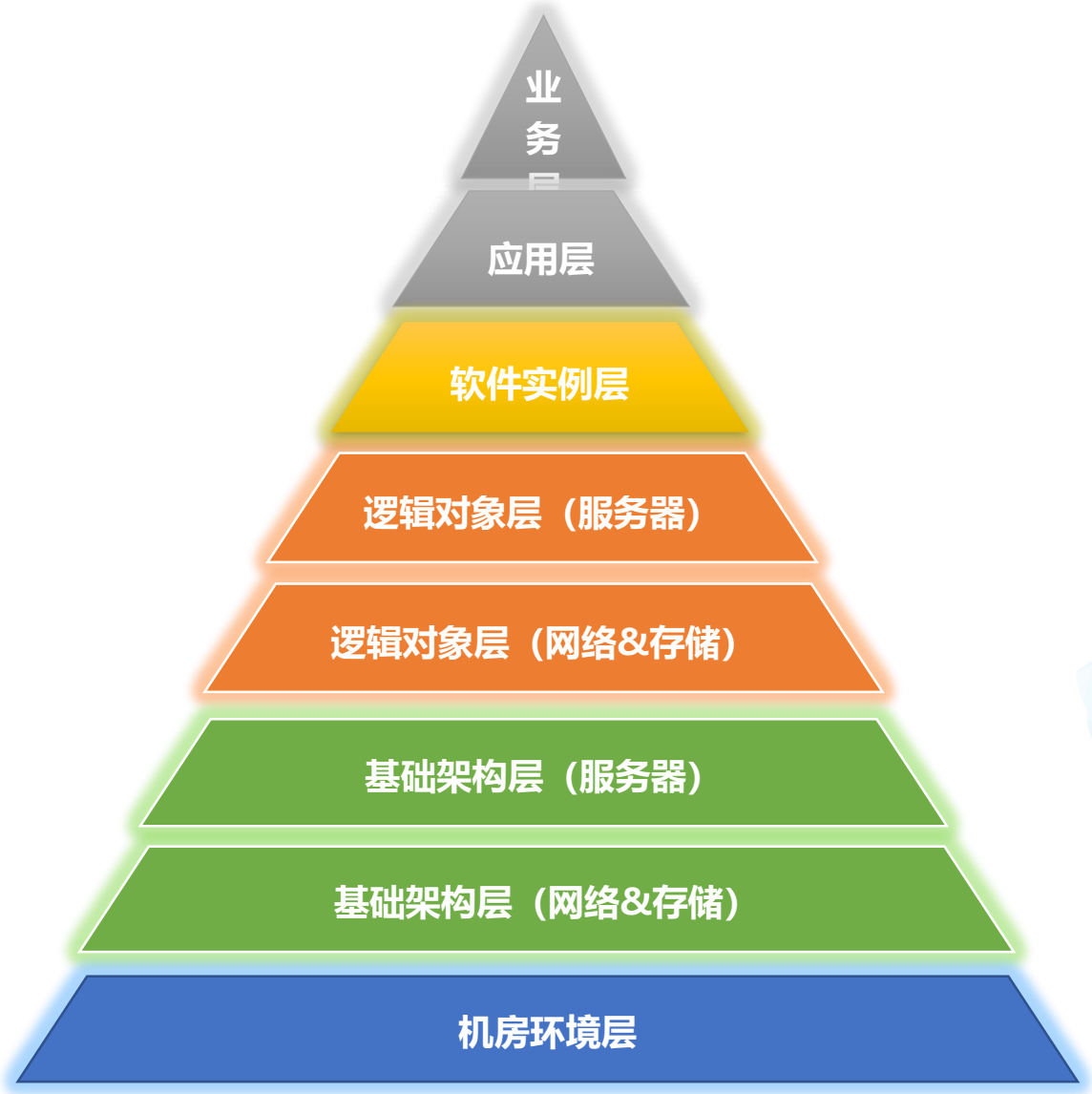
多平台信息融合

提高自动化水平

不断积累场景

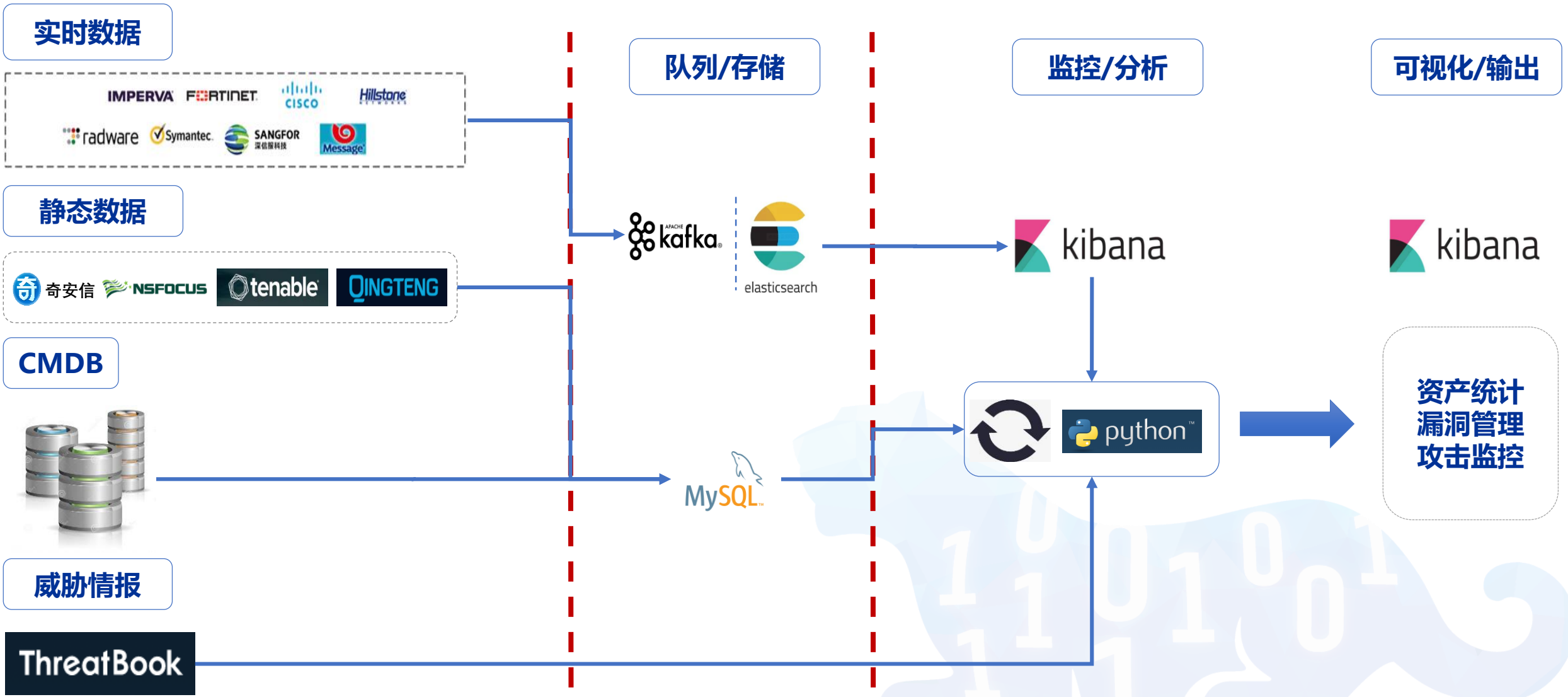
2 方案与实践

高价值的CMDB



业务	业务服务
应用	应用系统
软件实例	软件实例
逻辑对象	策略
	集群
	虚拟服务器
	逻辑存储单元
基础架构	物理服务器
	超融合
	机箱
	存储设备
	网络设备
	安全设备
	介质
	桌面
机房环境	机柜
	KVM
	电力辅助
	环境控制

多平台信息融合

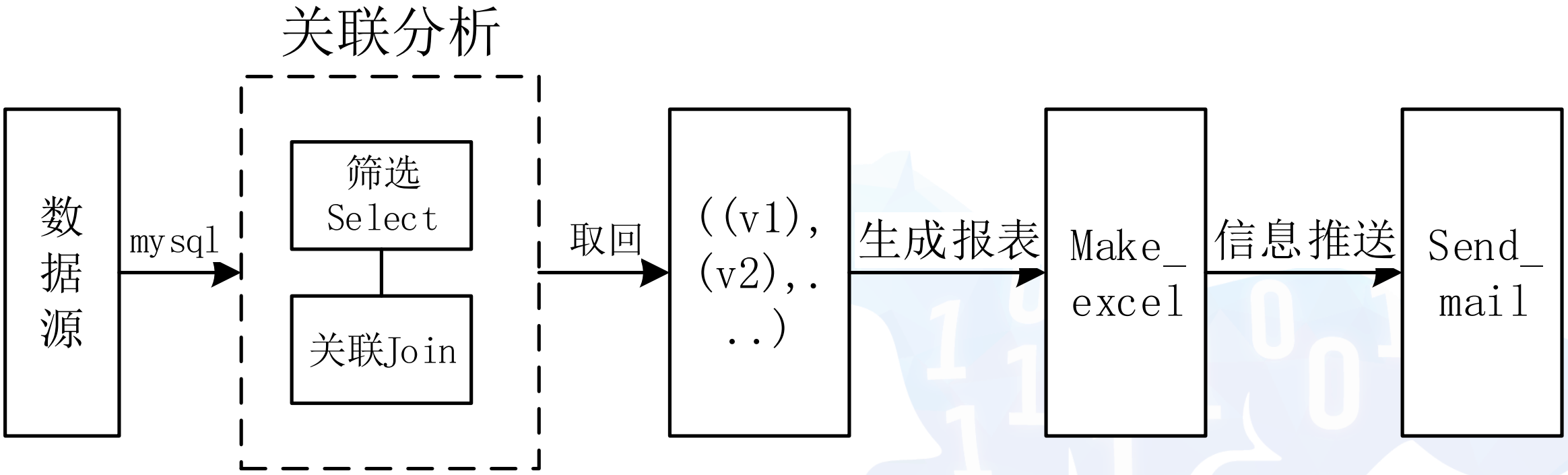

实时数据
IMPERVA
FORTINET
cisco
Hillstone
radware
Symantec.
SANGFOR
Message
静态数据
奇安信
NSFOCUS
tenable
QINGTENG
CMDB
威胁情报
ThreatBook
队列/存储
kafka
elasticsearch
MySQL
监控/分析
kibana
python
可视化/输出
kibana
资产统计
漏洞管理
攻击监控

核心组件

1. **静态基础数据库：** MYSQL
2. **外部工具：** 威胁情报，Tenable SCCV，绿盟扫描器等具备API的安全系统
3. **实时数据环境：** 利用kafka分布式订阅系统、Elasticsearch搜索引擎作为基础数据环境
4. **数据可视化：** Kibana及其开源插件sentinl，vega
5. **关联处理和信息转换：** python开发中间处理过程，完成关联交互和信息转出的步骤

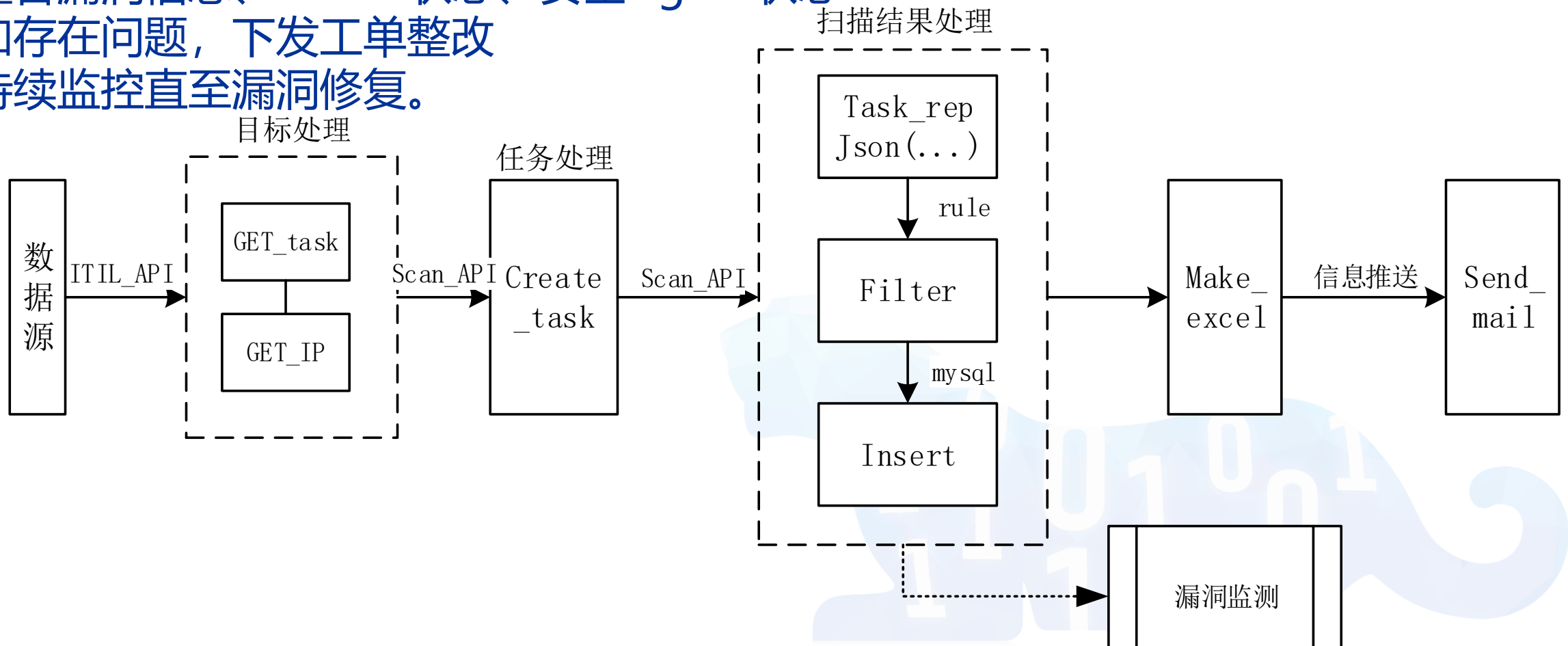
漏洞的持续监测

对漏洞库每周快照之间的比对分析，来持续监测漏洞变化，自动化得得出漏洞修复情况再关联CMDB资产库中的负责人信息，以工单或邮件通知安全负责人进行工单处理。



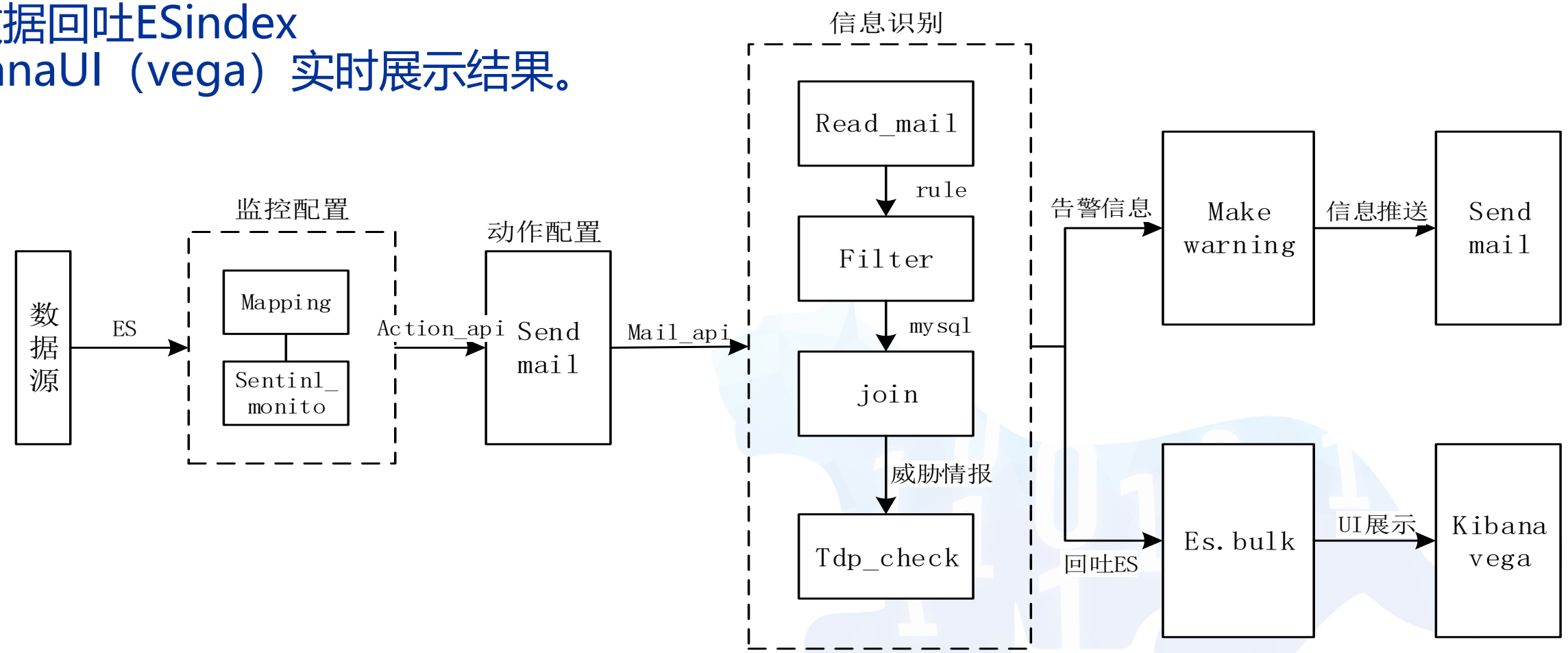
漏洞的流程化处理

1. 通过ITIL上线流程接口，获得新设备信息
2. 结合漏洞扫描器任务接口自动下发扫描任务
3. 整合漏洞信息、CMDB状态、安全Agent状态
4. 如存在问题，下发工单整改
5. 持续监控直至漏洞修复。



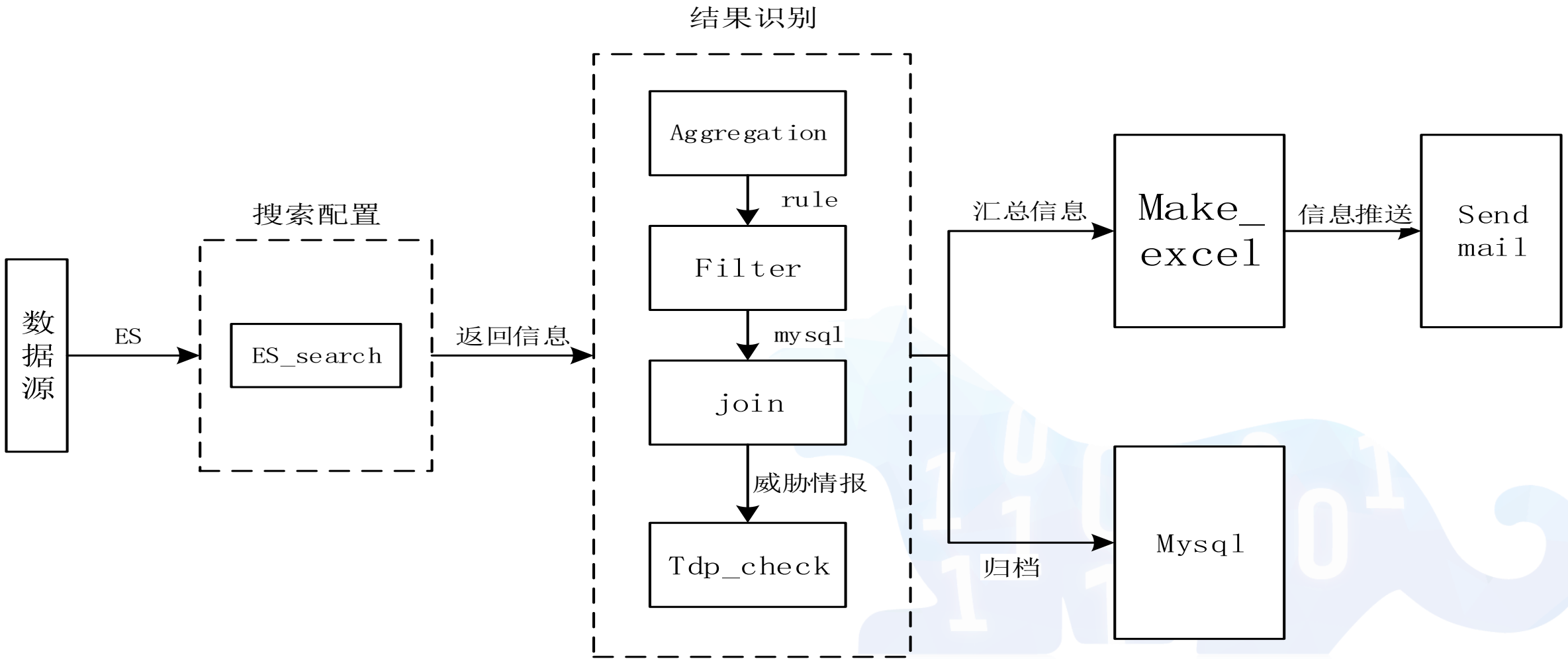
实时威胁发现

1. 安全实时日志集中至ESindex保存，做好mapping设计
2. Kibana插件Sentinl配置实时触发的告警规则和动作
3. 提取关键信息进行SQL关联分析和威胁情报关联，获得结果后数据回吐ESindex
4. KibanaUI（vega）实时展示结果。



每日报表

每日对ESindex中数据按照安全维度进行分类统计，将每日攻击情况和相关信息发送至安全负责人

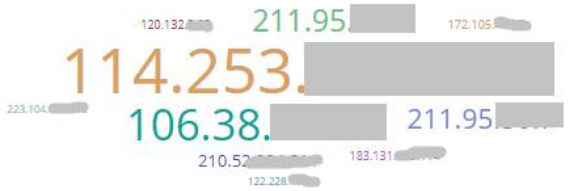


实时威胁发现

tag cloud:WAF src country [ArcSight]

tag cloud:WAF src city [ArcSight]

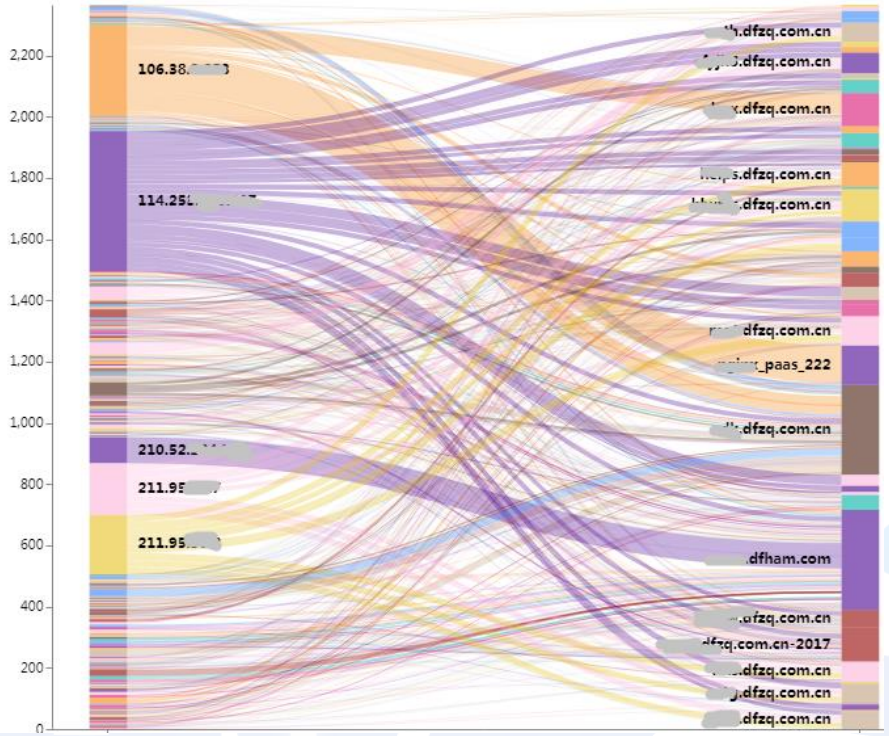
tag cloud:WAF src ip [ArcSight]



tag cloud:WAF event name [ArcSight]

The container is too small to display the entire cloud. Tags might be cropped or omitted.

Sankey waf sourceAddress to serverGroup



3 收获与展望

收获

- 提高管理效率
- 节省安全人力
- 提高安全发现与威胁响应能力

展望

不断完善CMDB内容

形成基于多维度的资产风险图谱

实现自动化和智能化运维


2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE
THANKS!