日志实时分析@安全

罗启武，携程信息安全中心

恶意请求（机器）

攻击尝试（应用/业务）

恶意请求

- 恶意抓数据
- 恶意注册/登陆/扫号
- 恶意扫描/CC
- 秒杀/抢票
- 发垃圾信息
- 资源占用

攻击尝试

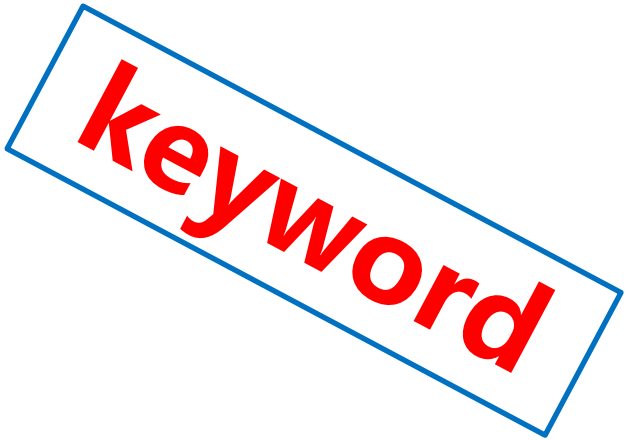
- 恶意扫描
- 安全测试
- 应用漏洞
- 逻辑漏洞

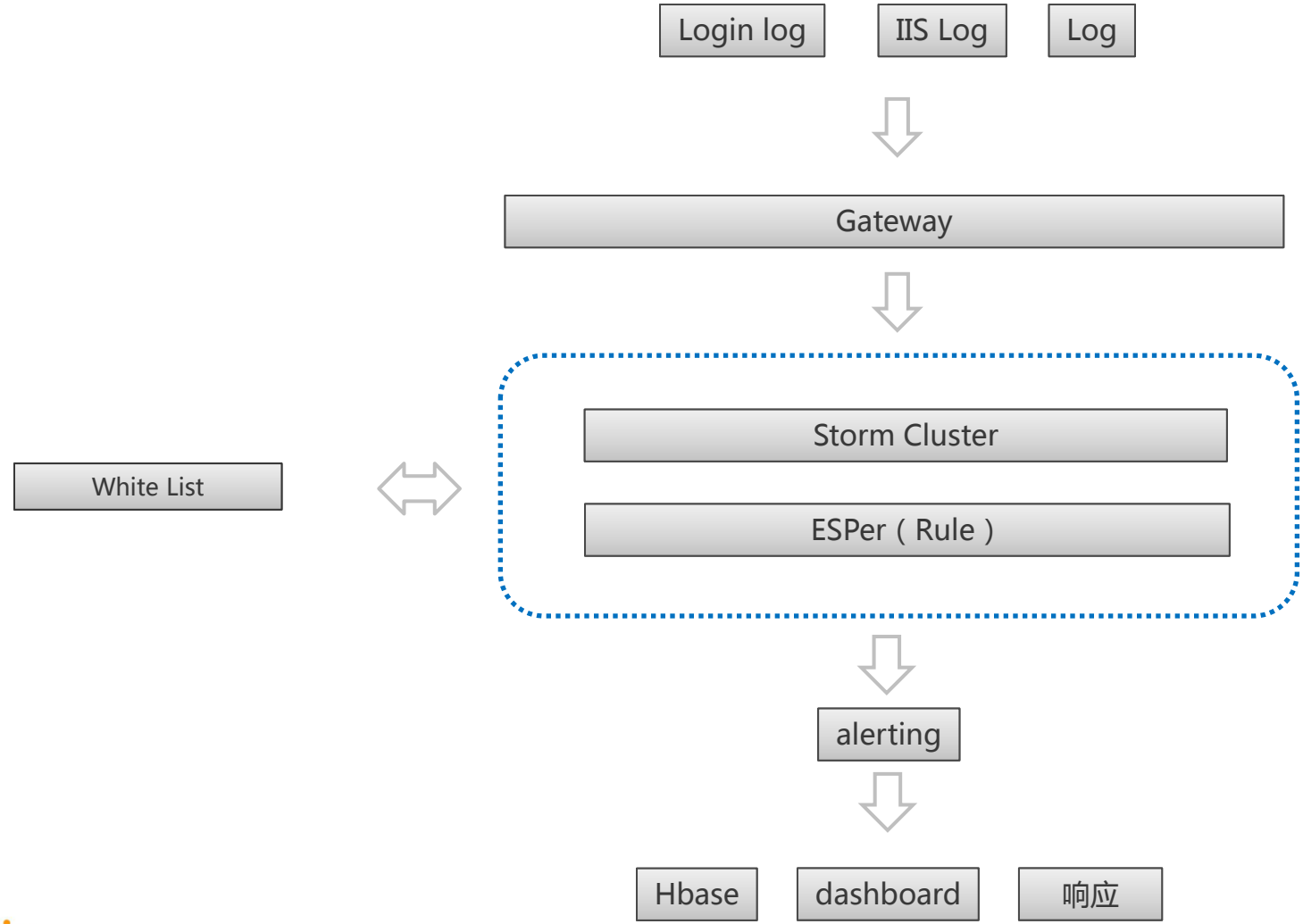
实时

稳定

处置

dashboard




Login log
IIS Log
Log
Gateway
Storm Cluster
ESPer (Rule)
White List
alerting
Hbase
dashboard
响应

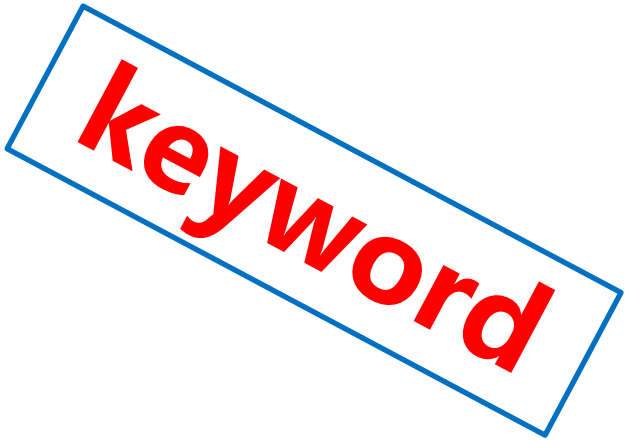
规则配置化

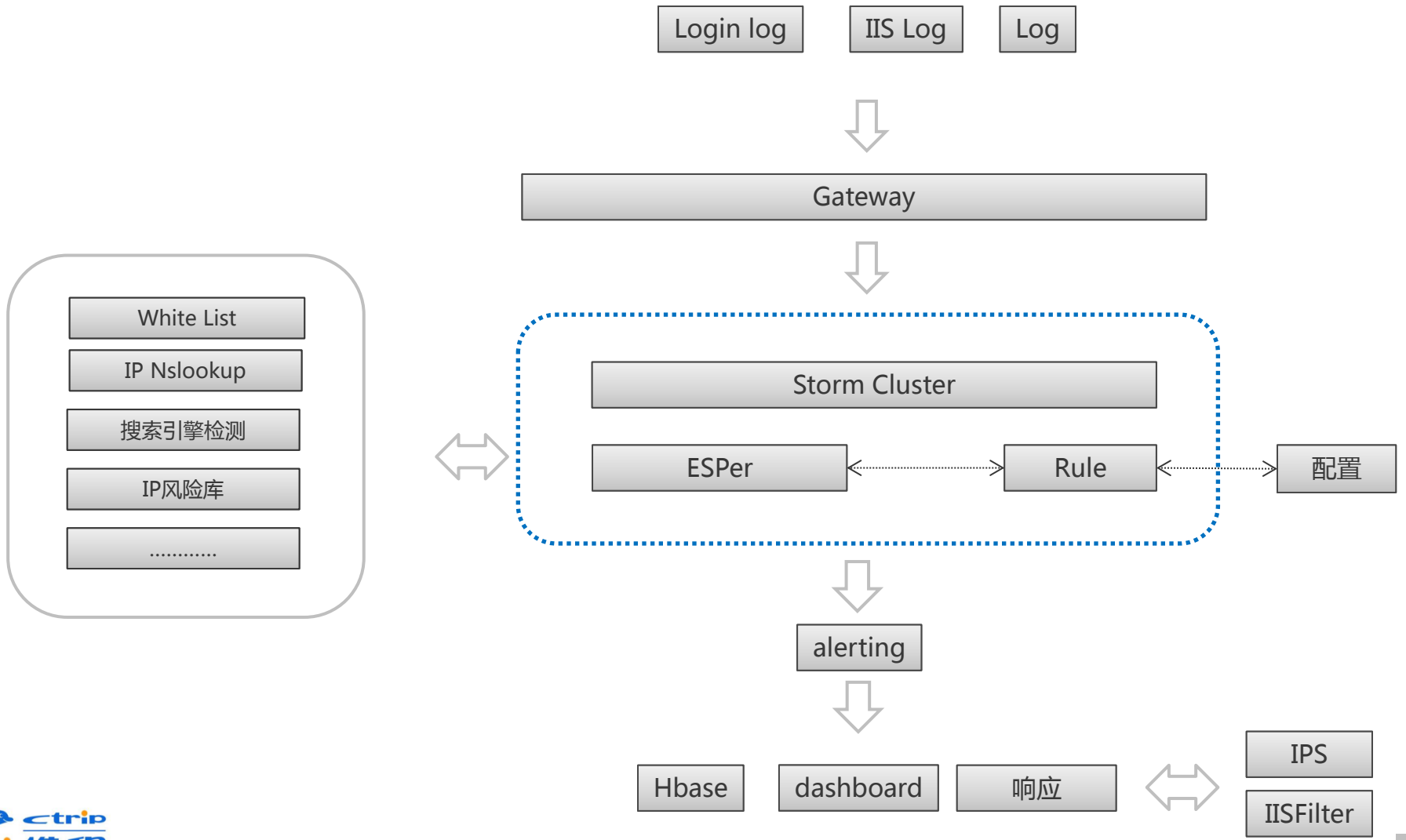
逻辑

辅助数据

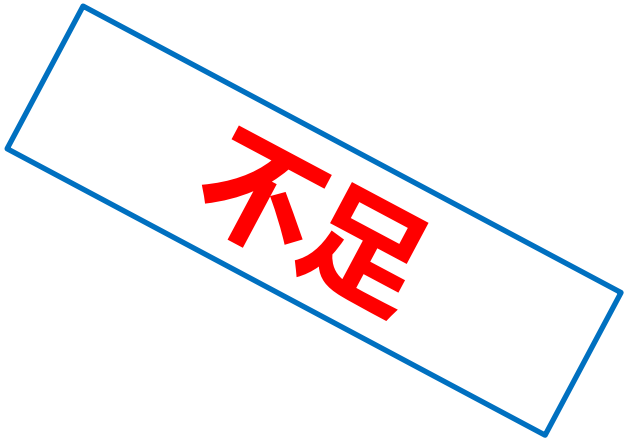
误杀率

dashboard




Login log
IIS Log
Log
Gateway
White List
IP Nslookup
搜索引擎检测
IP风险库
.....
Storm Cluster
ESPer
Rule
配置
alerting
Hbase
dashboard
响应
IPS
IISFilter

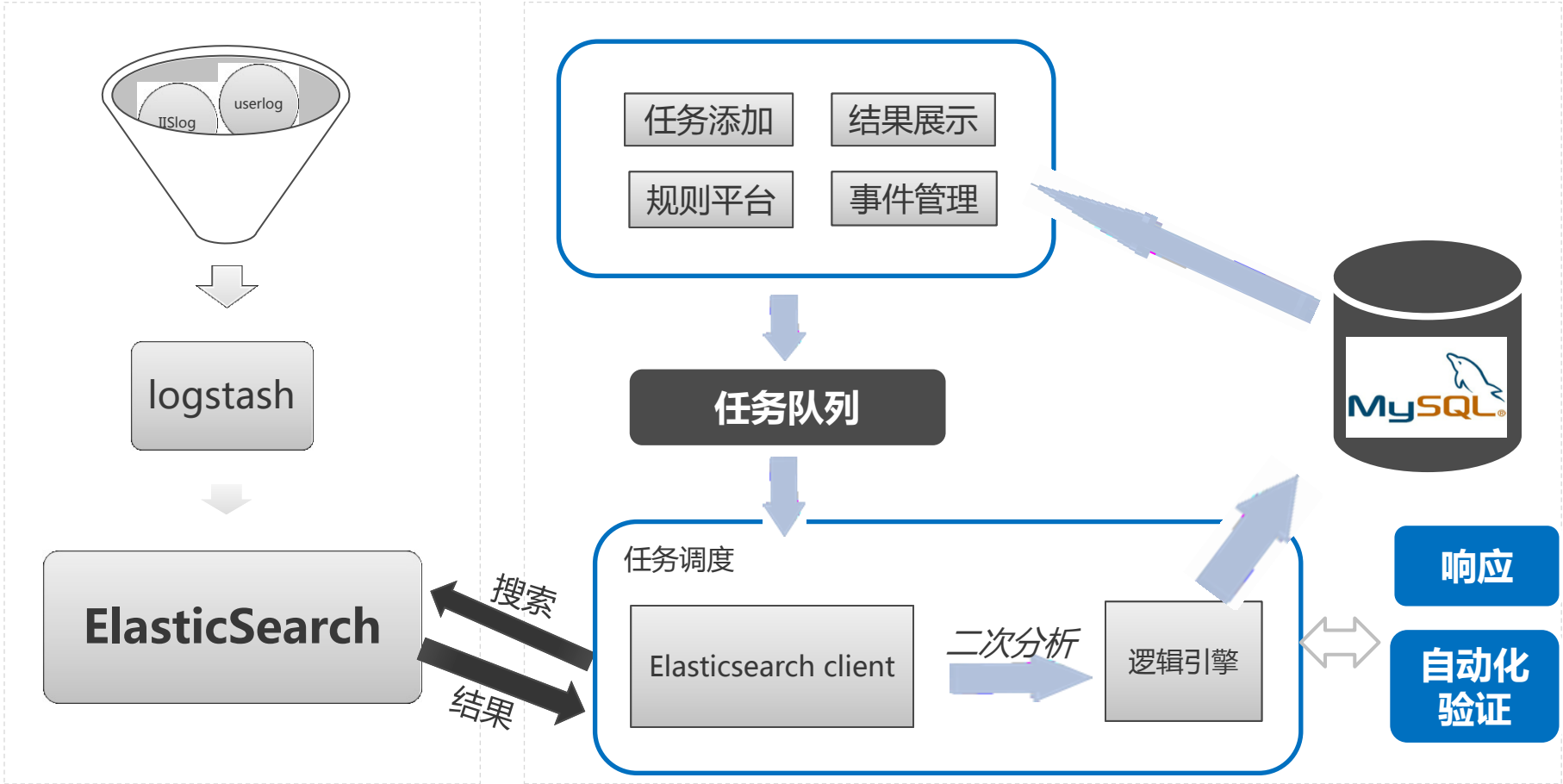
- 纯内存
- 时间窗口
- 逻辑规则
- 误杀率
- 离线学习



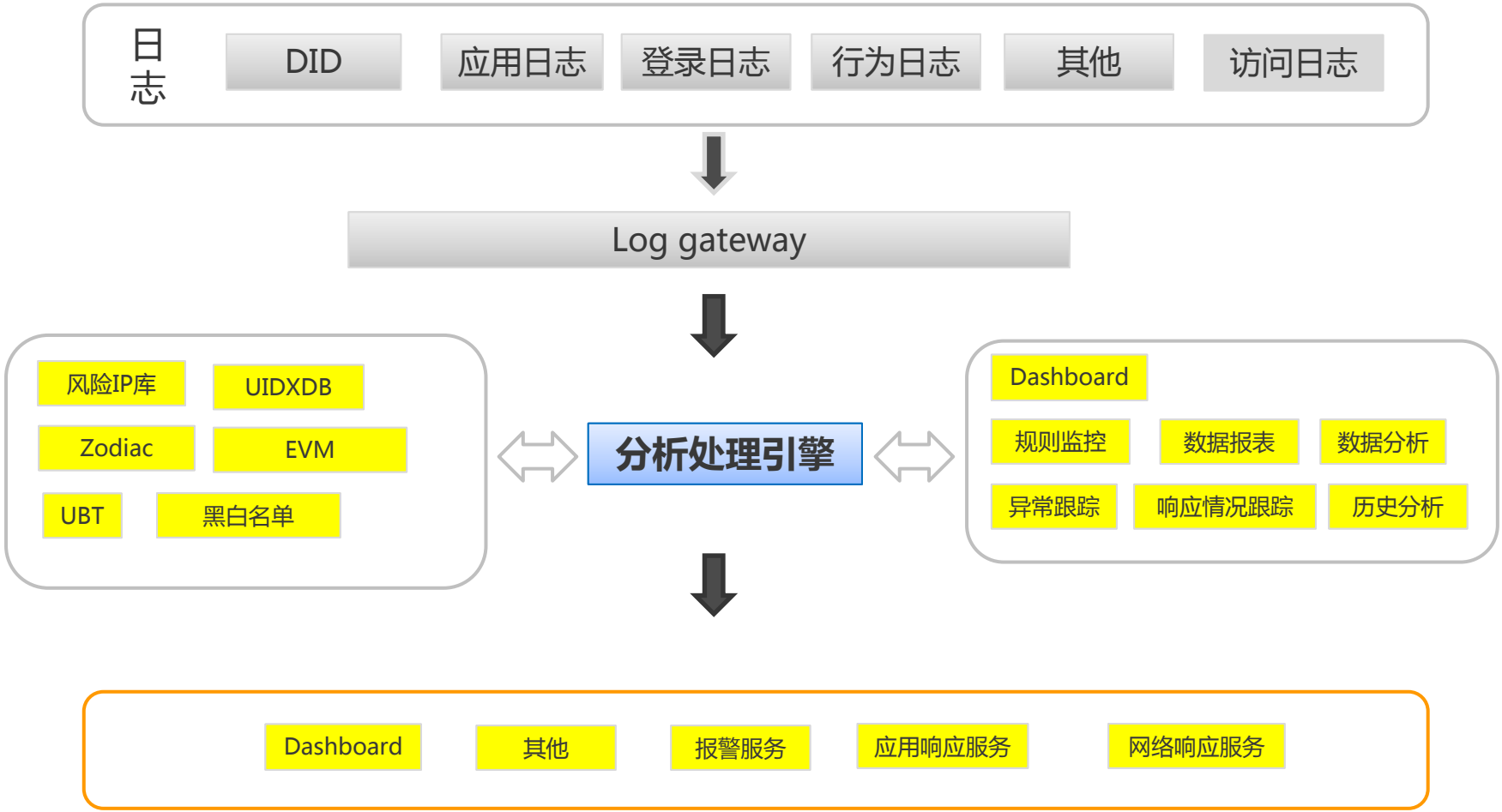
Splunk

Elasticsearch

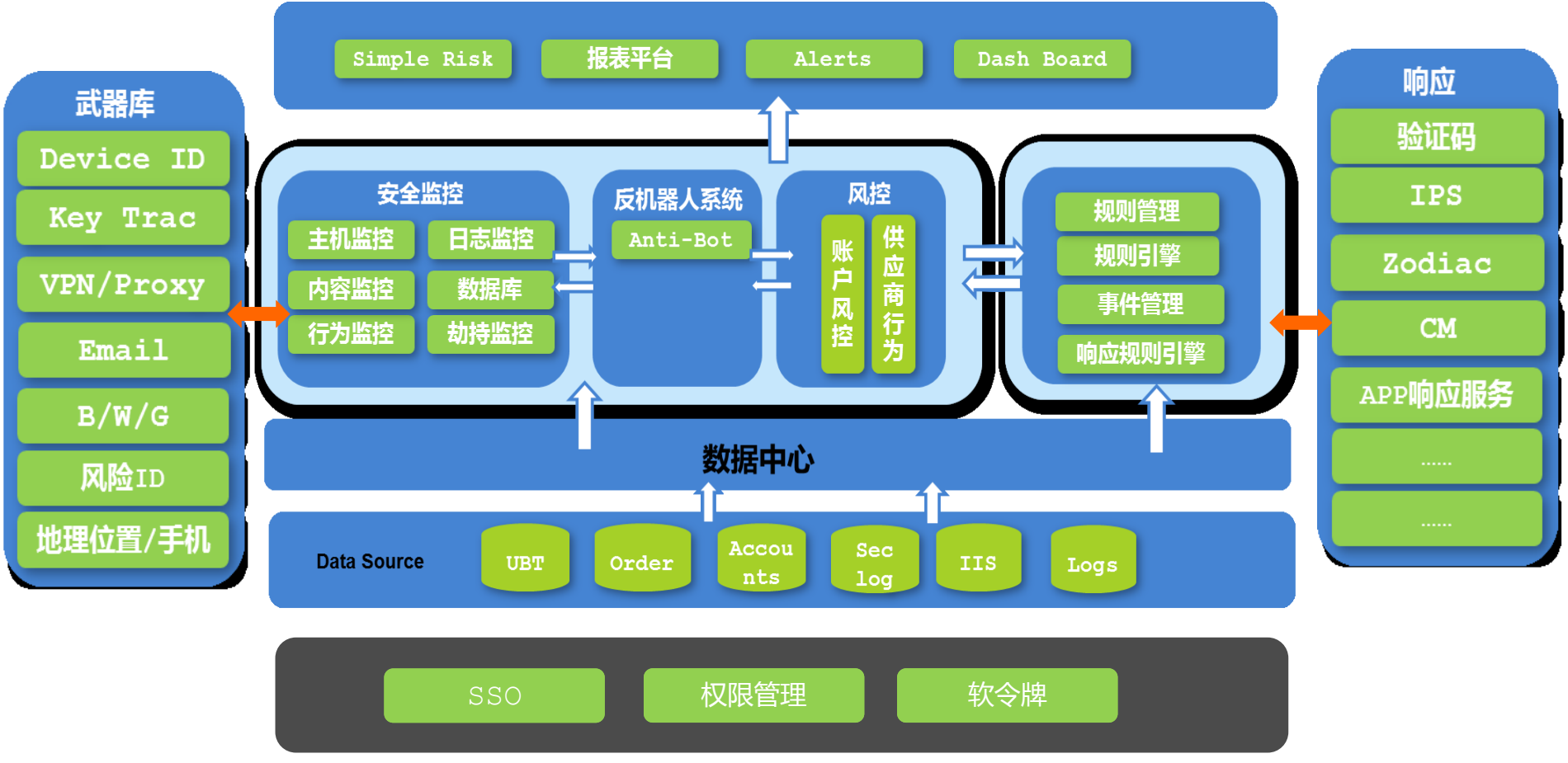
ESlog


IISlog
userlog
logstash
ElasticSearch
搜索
结果
任务添加
结果展示
规则平台
事件管理
任务队列
任务调度
Elasticsearch client
二次分析
逻辑引擎
MySQL
响应
自动化
验证

规划


日志
DID
应用日志
登录日志
行为日志
其他
访问日志
Log gateway
风险IP库
UIDXDB
Zodiac
EVM
UBT
黑白名单
分析处理引擎
Dashboard
规则监控
数据报表
数据分析
异常跟踪
响应情况跟踪
历史分析
Dashboard
其他
报警服务
应用响应服务
网络响应服务

安全产品规划


Simple Risk
报表平台
Alerts
Dash Board
武器库
Device ID
Key Trac
VPN/Proxy
Email
B/W/G
风险ID
地理位置/手机
安全监控
主机监控
日志监控
内容监控
数据库
行为监控
劫持监控
反机器人系统
Anti-Bot
风控
账户风控
供应商行为
规则管理
规则引擎
事件管理
响应规则引擎
响应
验证码
IPS
Zodiac
CM
APP响应服务
.....
.....
数据中心
Data Source
UBT
Order
Accounts
Sec log
IIS
Logs
SSO
权限管理
软令牌

携程安全应急响应中心

sec.ctrip.com

Thanks

For your attention