

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/

攻击尝试

- 恶意扫描
- 安全测试

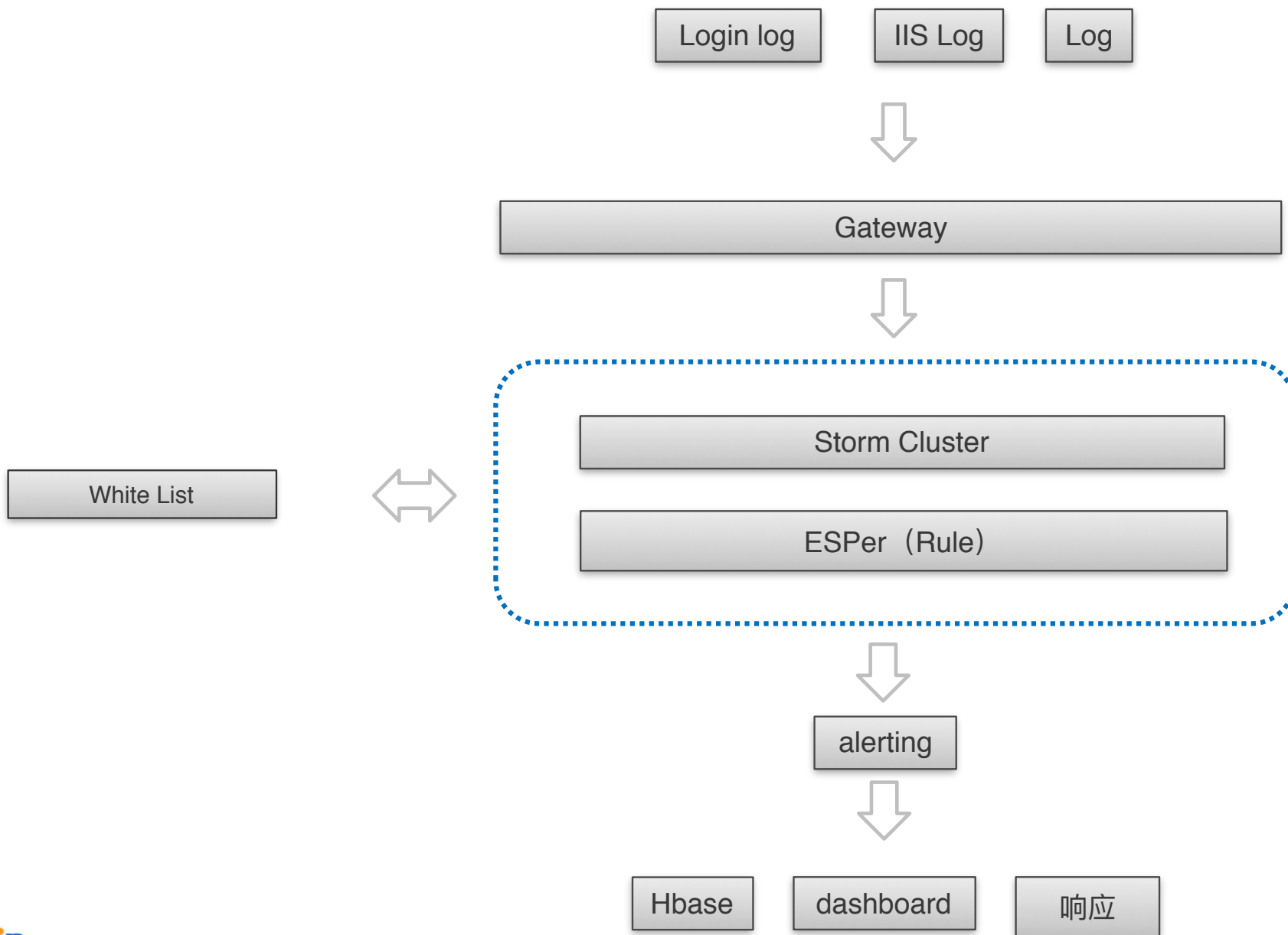
实时

稳定

处置

dashboard

keyword



规则配置化

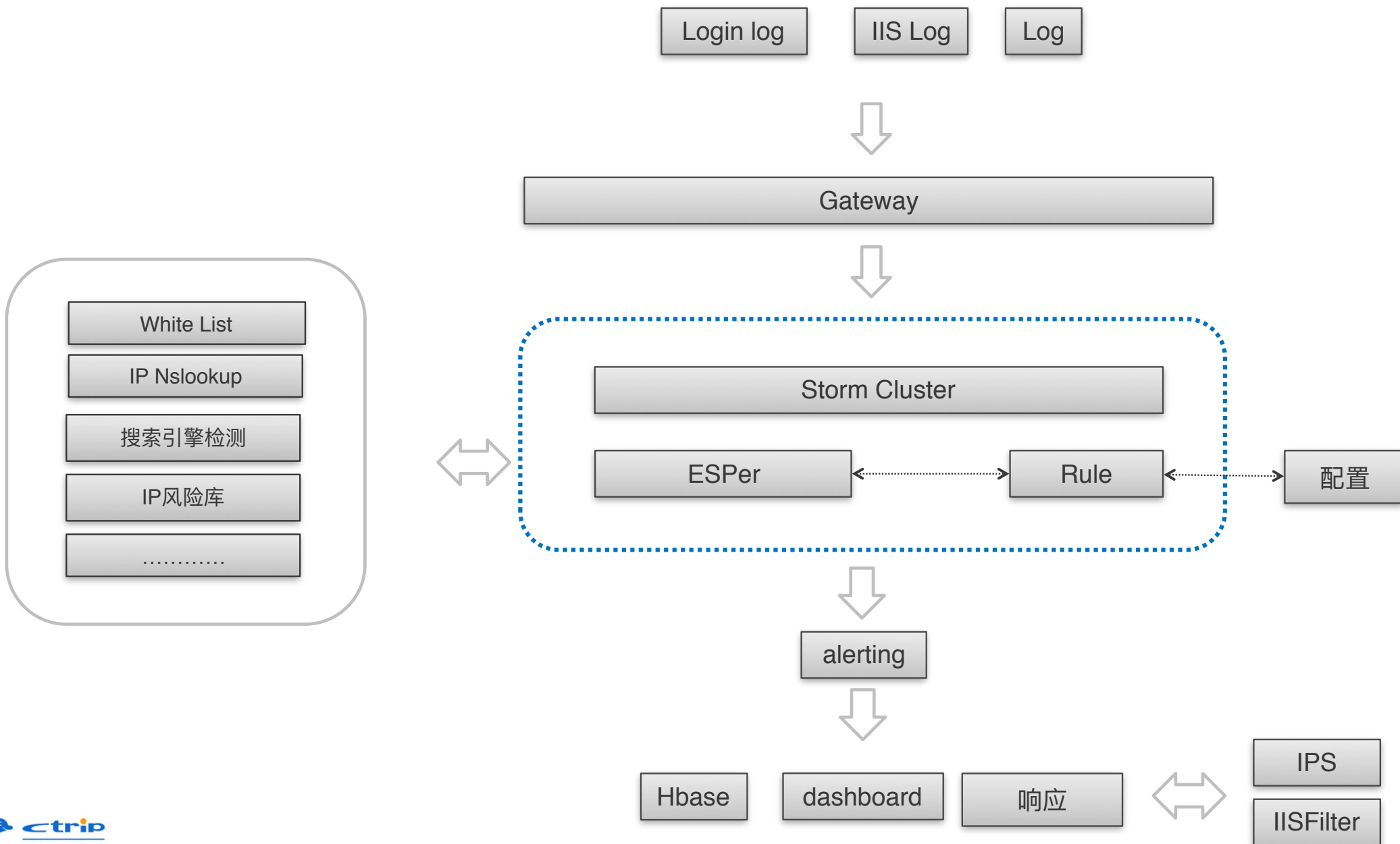
逻辑

辅助数据

误杀率

dashboard

keyword



纯内存

时间窗口

逻辑规则

误杀率

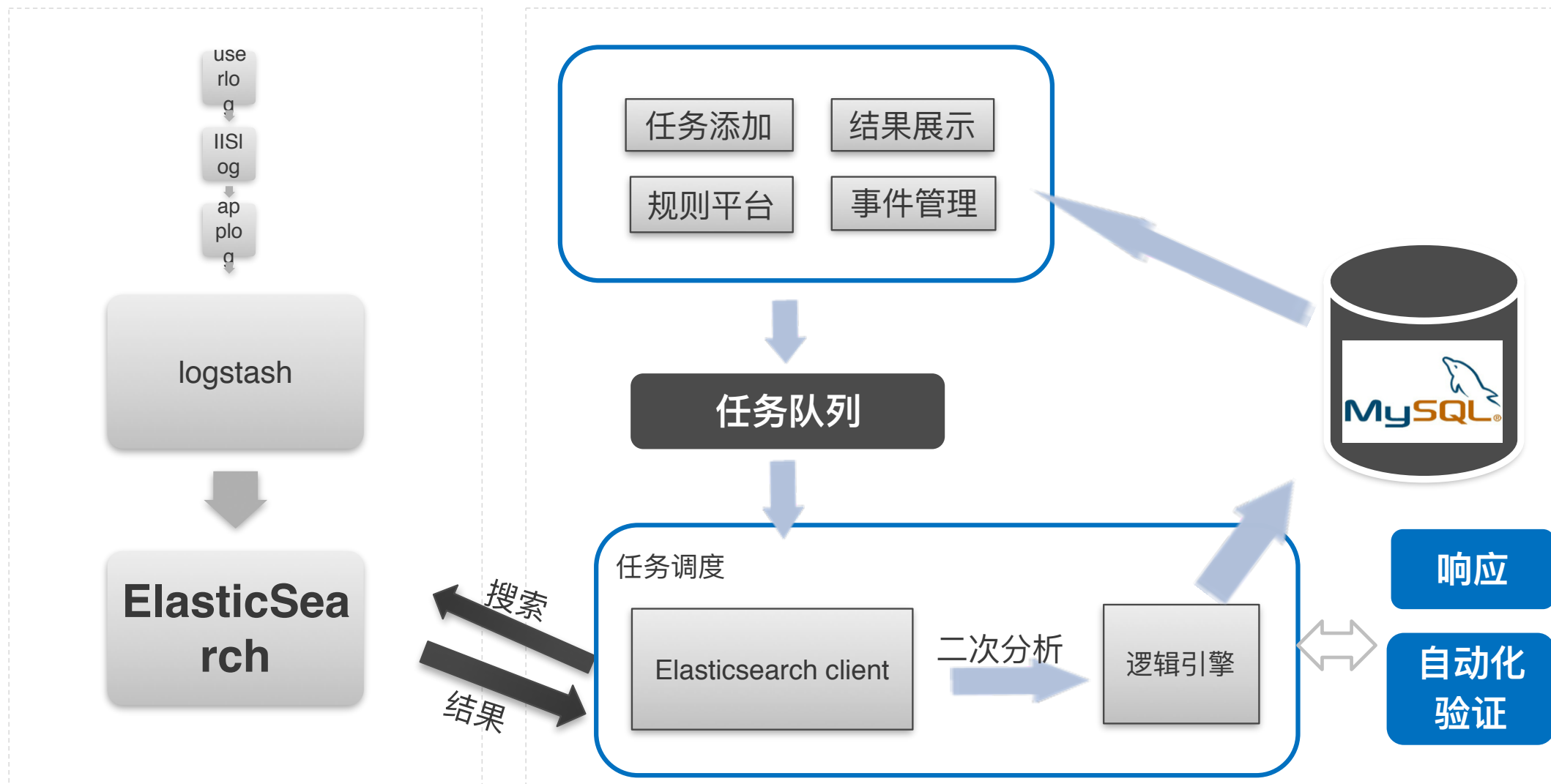
离线学习

不足

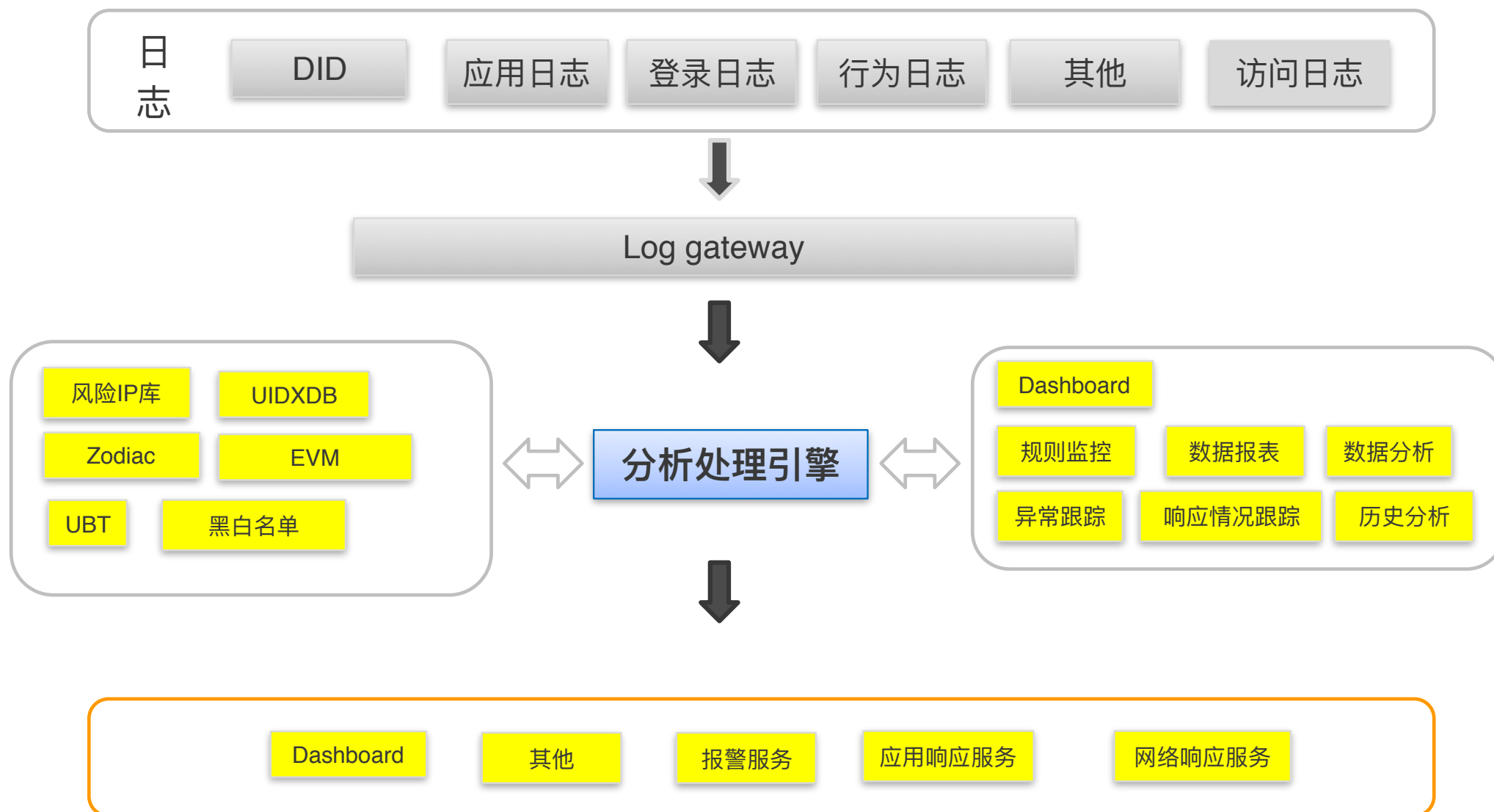
Splunk

Elasticsearch

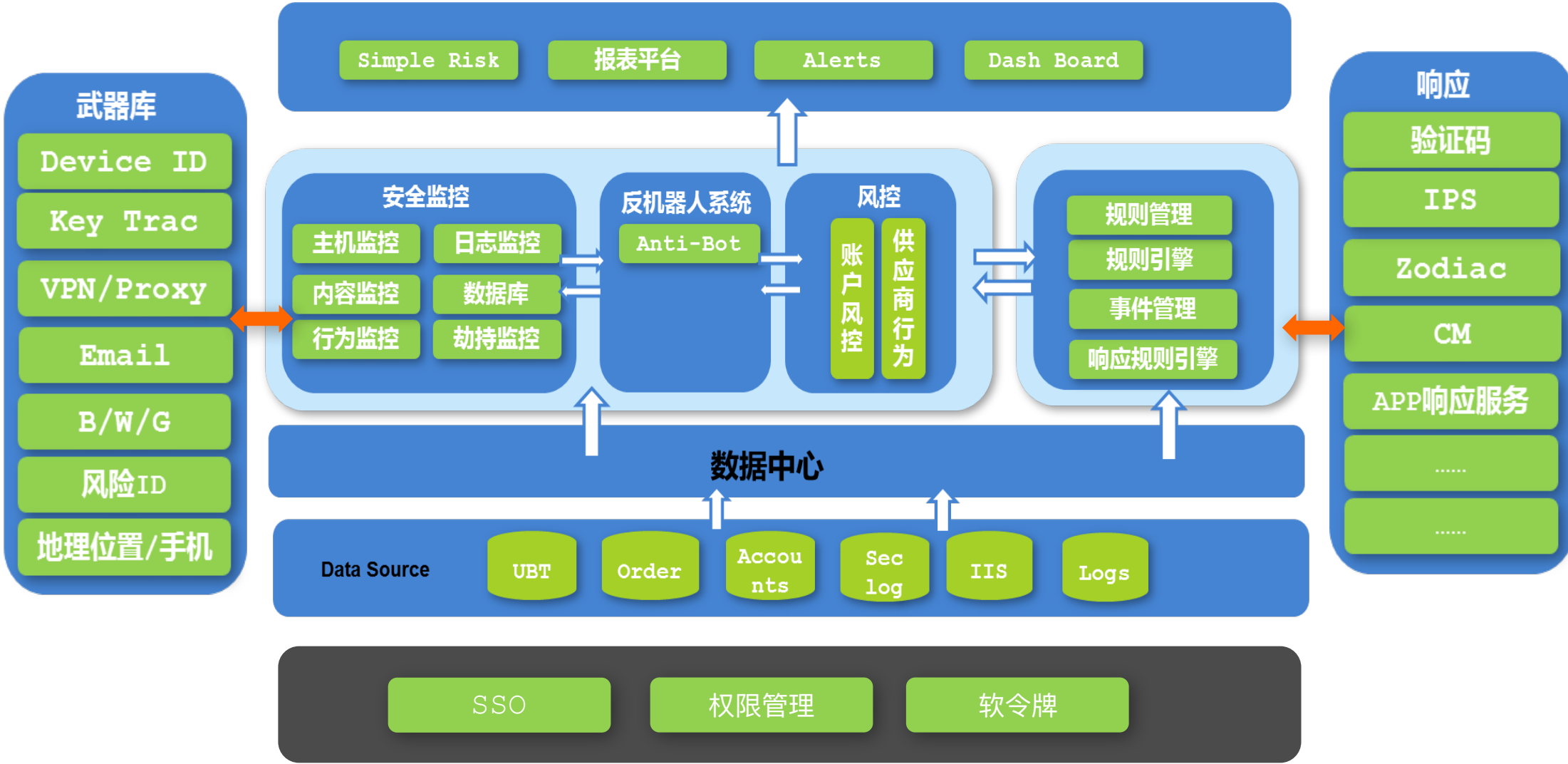
ESlog



规划



安全产品规划



携程安全应急响应中心
sec.ctrip.com



Thanks

For your attention