从防御到检测的企业安全之路

纪舒瀚 汽车之家

我是谁

姓名：纪舒瀚
公司：汽车之家
职位：安全负责人，团队及安全体系从0到1建设者

Autohome

论坛、电商、车金融、后市场

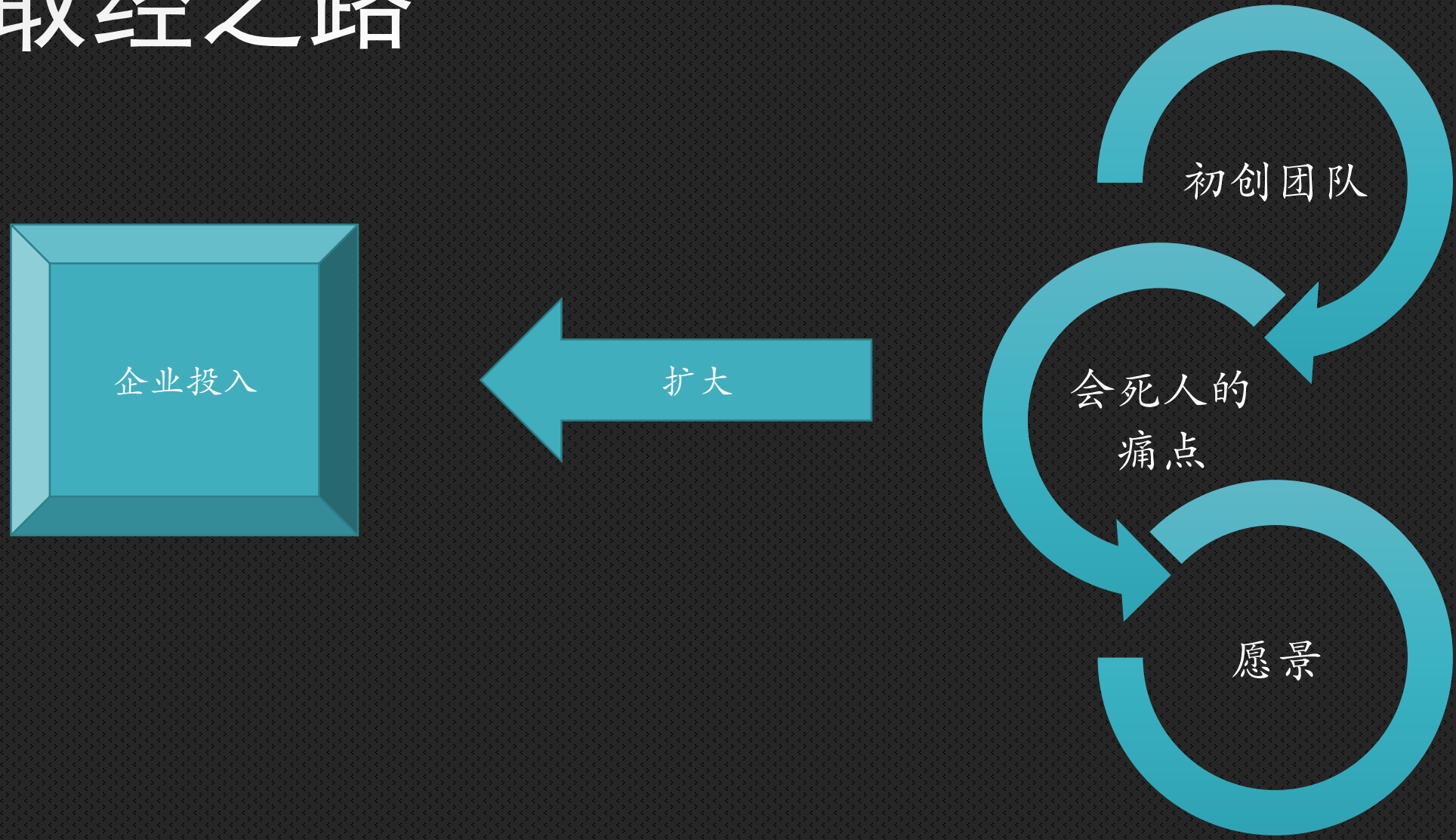
大纲

1、迷茫的需求
2、企业安全理解
3、一点案例
4、汽车之家安全实践

迷 茫

安全意愿≠安全需求

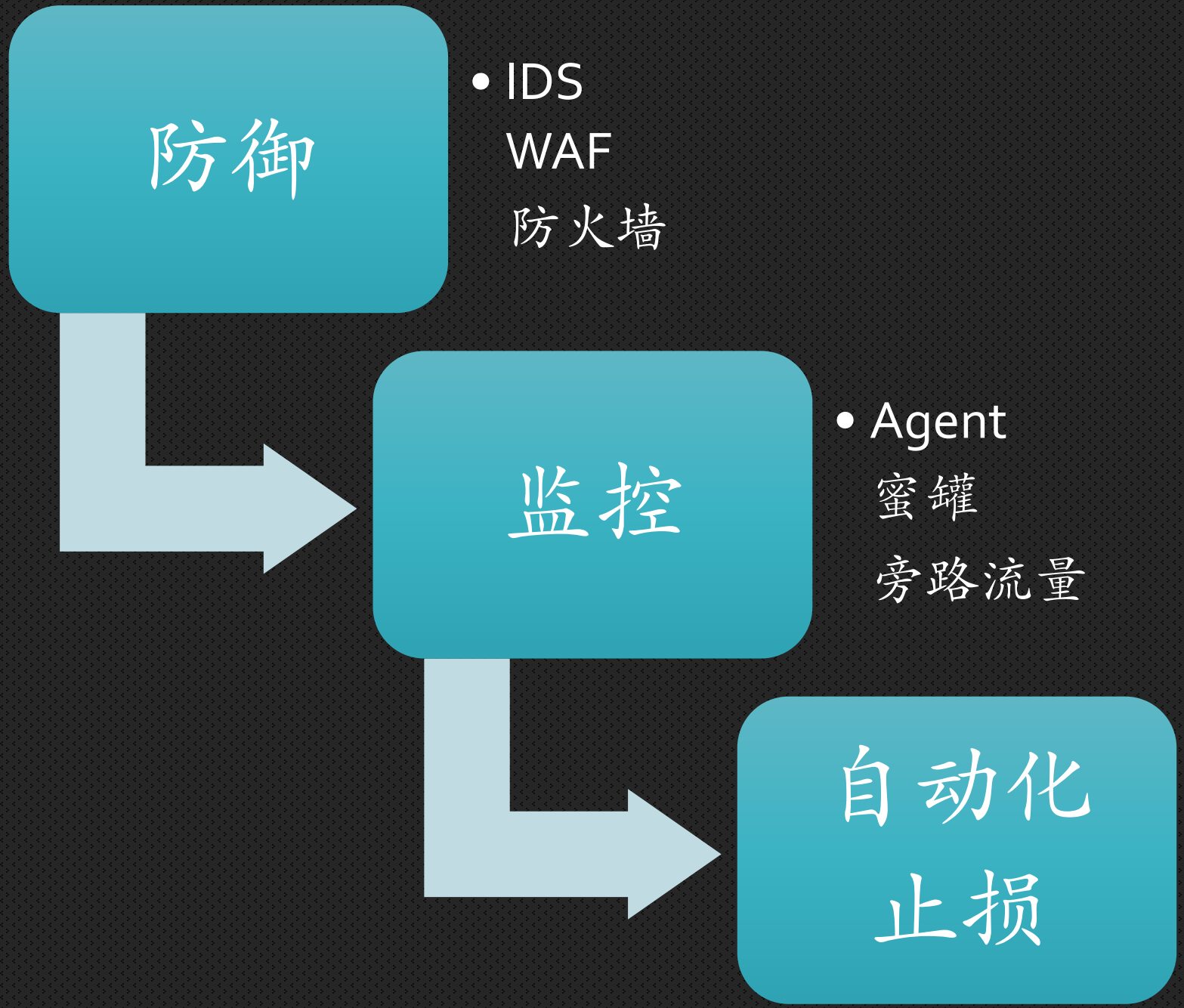
取经之路



谁也别想 占到便宜

提高　安全感知能力

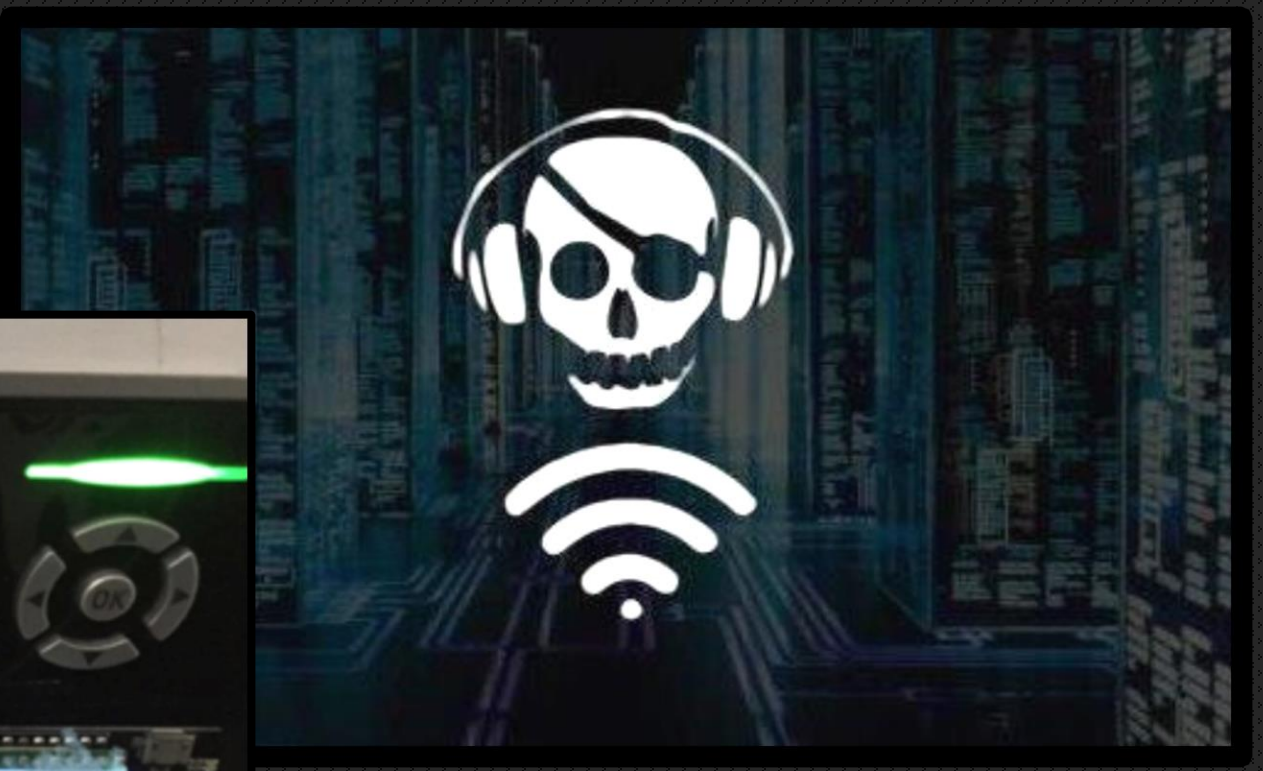
企业安全防护的变化


防御
• IDS
WAF
防火墙
监控
• Agent
蜜罐
旁路流量
自动化
止损
• TIP+SOC
资产空间可视化
固定资产、威胁
资产

新挑战


技术变化
边界变化
合规变化
业务需求变化
攻击变化

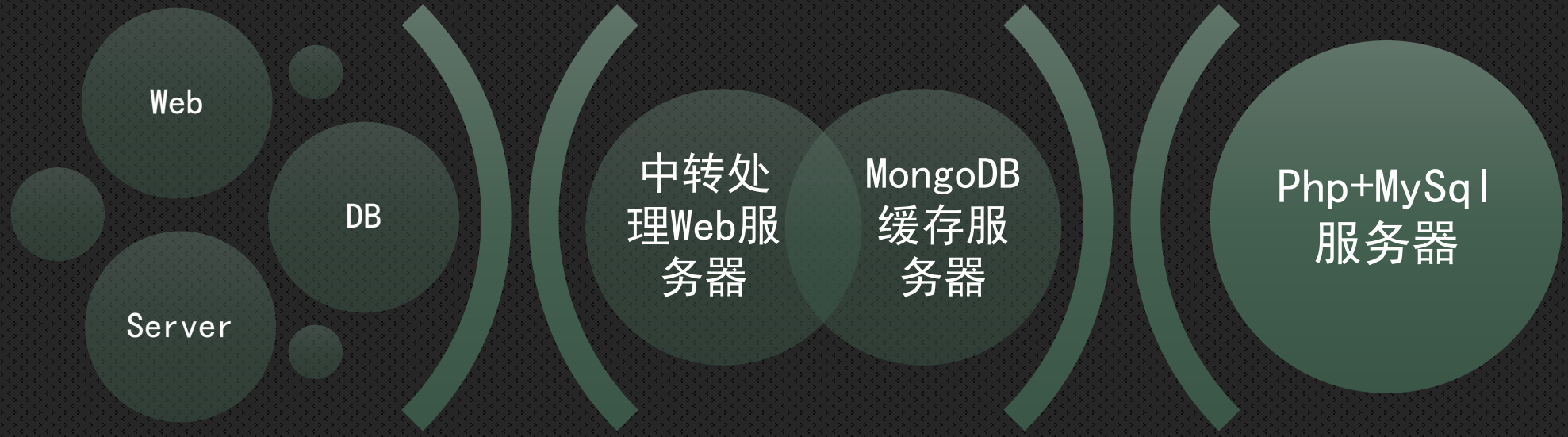
新边界




M880
OK

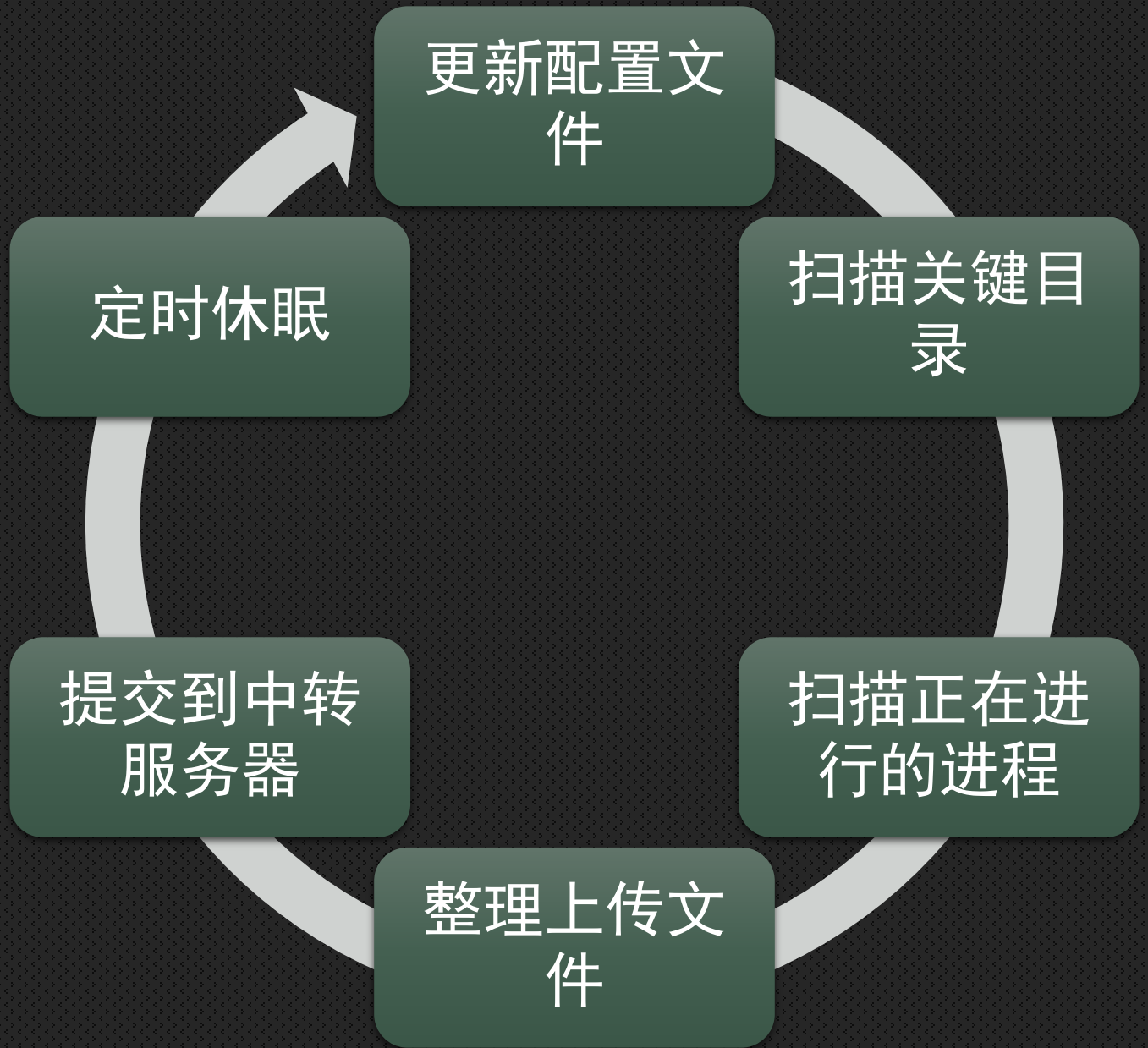
举个栗子

基本框架

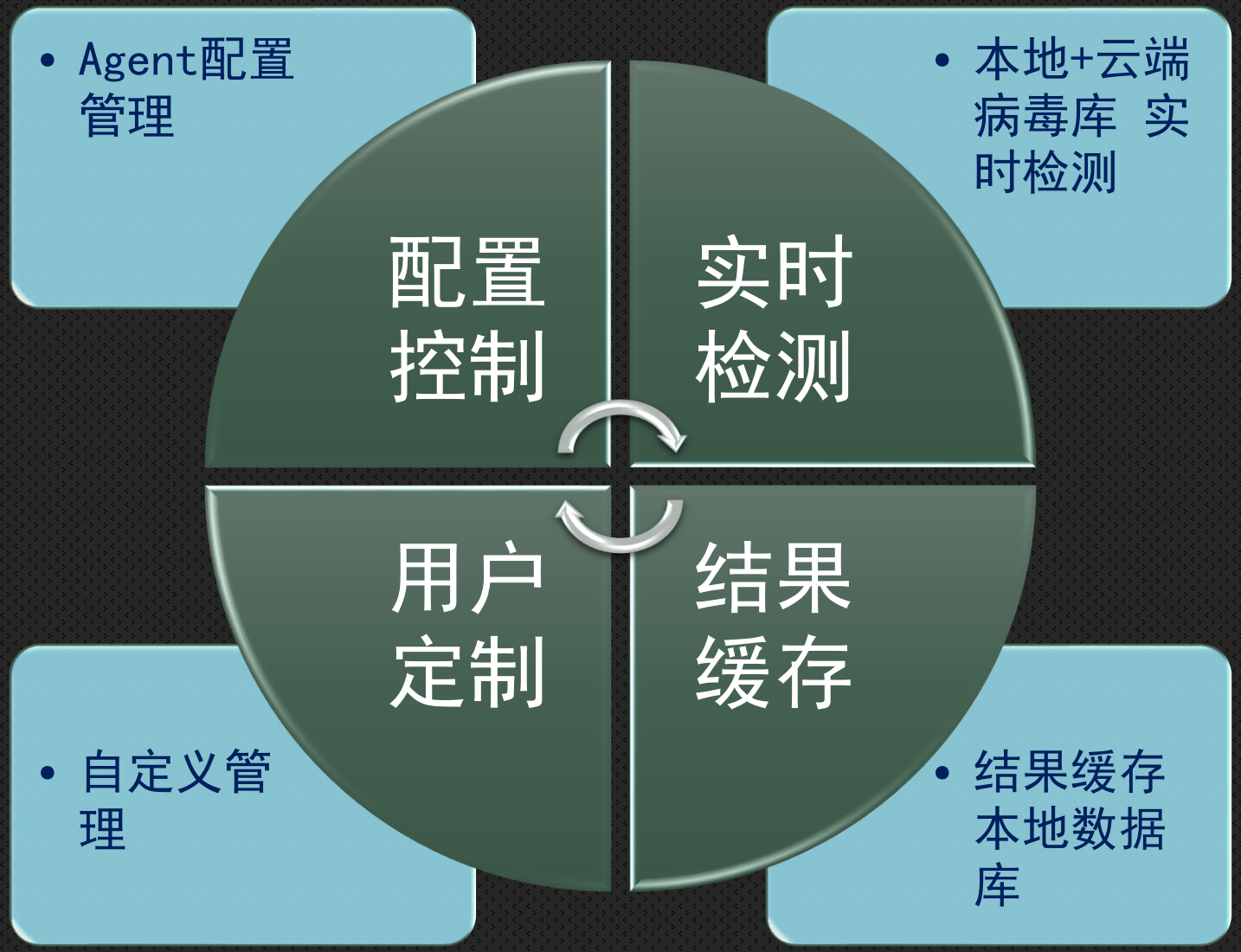


Agent端　　处理端　　SOC展示

Agent



中转服务器构成


• Agent配置管理
• 本地+云端病毒库 实时检测
配置控制
实时检测
用户定制
结果缓存
• 自定义管理
• 结果缓存本地数据库

中转处理结果升级

白名单文件

本地病毒库

云端病毒库

病毒沙箱模拟运行结果

处理效率

Agent端

- 15分钟增量扫描
- 30天全盘扫描

中转

- 实时检测Agent提交的数据
- 60天本地病毒库更新

我们的实践


终端 + 镜像
安全态势可视化
业务安全现状报表
安全策略效果报表
武器库策略优化
业务输出
内部威胁分析
外部威胁分析
关联溯源分析
预测分析
数据采集
多源格式化数据
代码安全工具
沙箱
边界监控
蜜罐
报警机制
终端响应机制

我们的交付

威胁的先扬后抑，寻找对抗的平衡点

谢谢