百万级服务器反入侵场景的混沌工程实践

黄兆楠

高级工程师

Geekbang. 极客邦科技 InfoQ

极客邦科技
会议推荐2019

5月

QCon 北京
全球软件开发大会
大会：5月6–8日
培训：5月9–10日

QCon 广州
全球软件开发大会
培训：5月25–26日
大会：5月27–28日

6月

GTLC GLOBAL TECH LEADERSHIP CONFERENCE 上海
技术领导力峰会
时间：6月14–15日

GMTC 北京
全球大前端技术大会
大会：6月20–21日
培训：6月22–23日

7月

ArchSummit 深圳
全球架构师峰会
大会：7月12–13日
培训：7月14–15日

10月

QCon 上海
全球软件开发大会
大会：10月17–19日
培训：10月20–21日

11月

GMTC 深圳
全球大前端技术大会
大会：11月8–9日
培训：11月10–11日

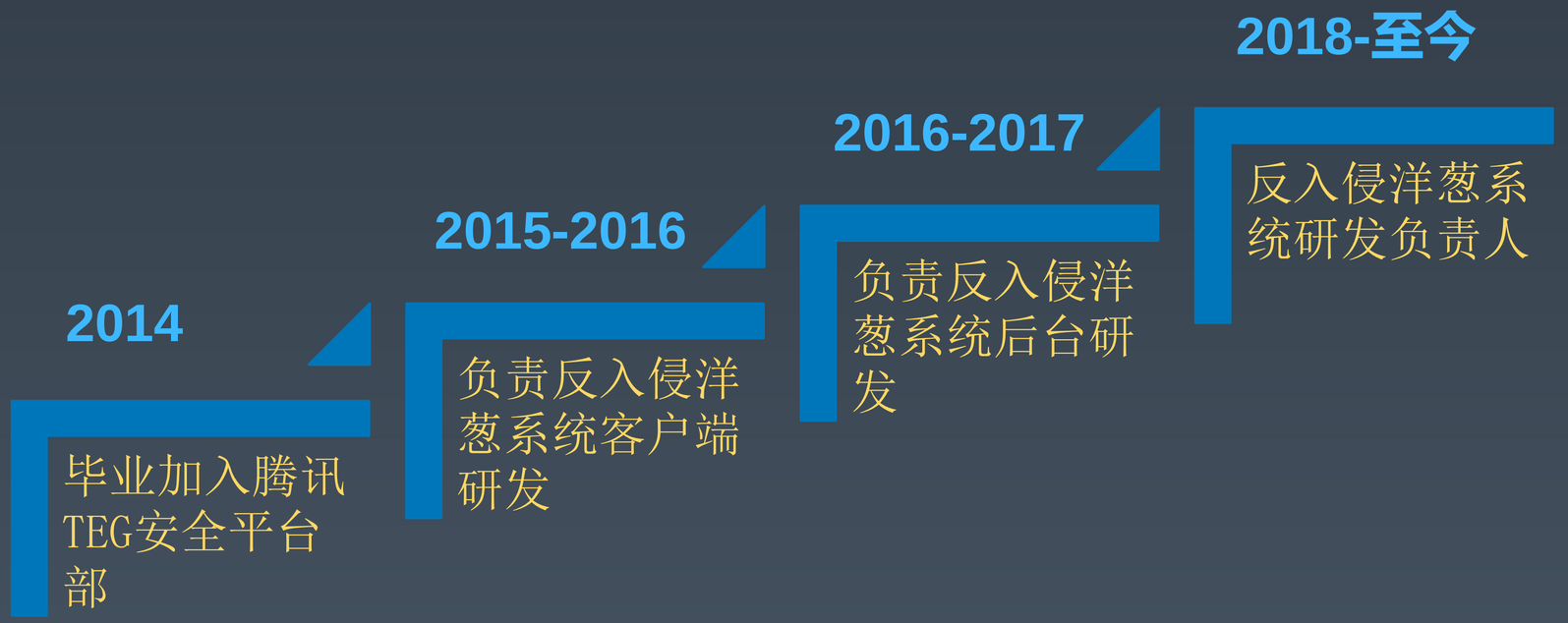
AiCon 北京
全球人工智能与机器学习大会
大会：11月21–22日
培训：11月23–24日

12月

ArchSummit 北京
全球架构师峰会
大会：12月6–7日
培训：12月8–9日

自我介绍

黄兆楠： 腾讯TEG安全平台部 反入侵洋葱系统研发负责人

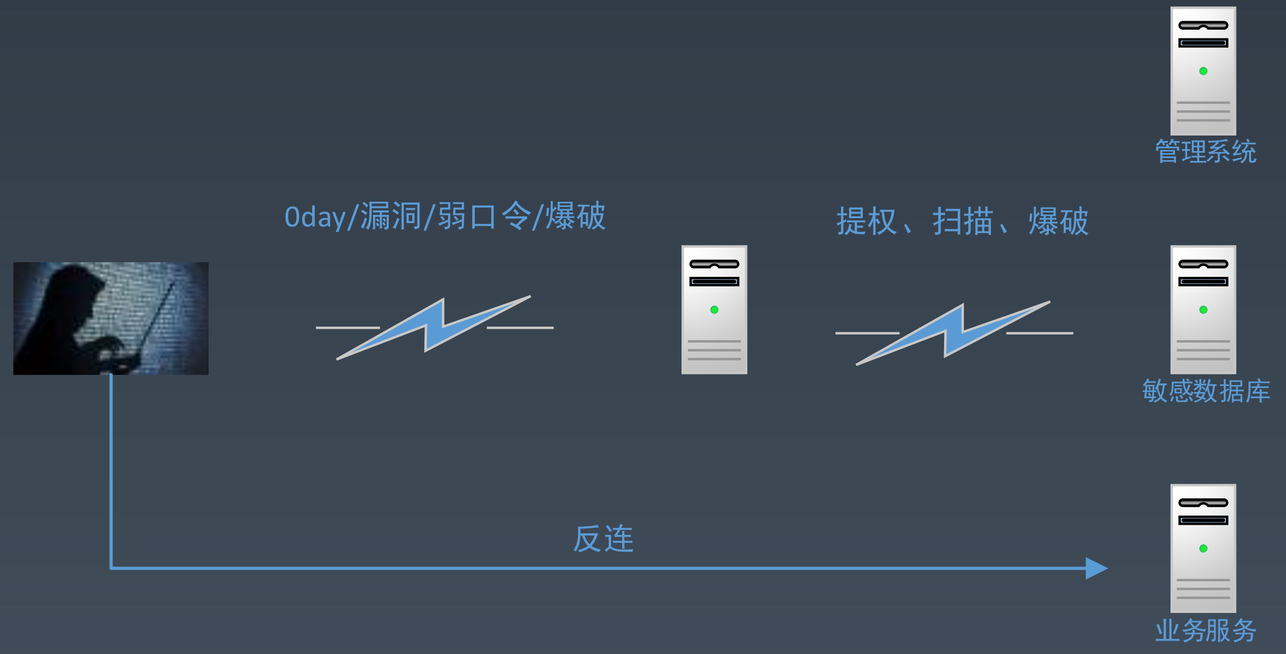


目录

- 介绍反入侵洋葱系统及面临的挑战
- 复杂规模下的质量建设思路
- 反入侵场景下的混沌实践
- 总结展望

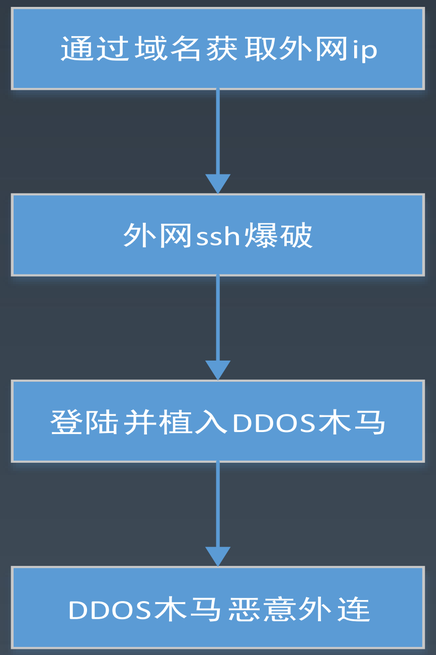
什么叫“入侵”

- 未经授权
- 获取敏感数据（如关系链信息，用户信息）
- 篡改数据（如恶意删除，给自己充钱，主页篡改）
- 控制资产（让服务器对外发起ddos、当作渗透其它目标的跳板、跑个比特币挖矿程序等）

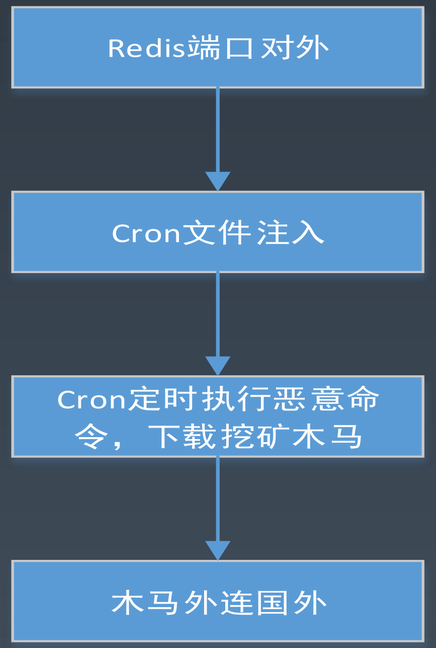


从历史入侵case出发

腾讯云上服务被植入ddos木马



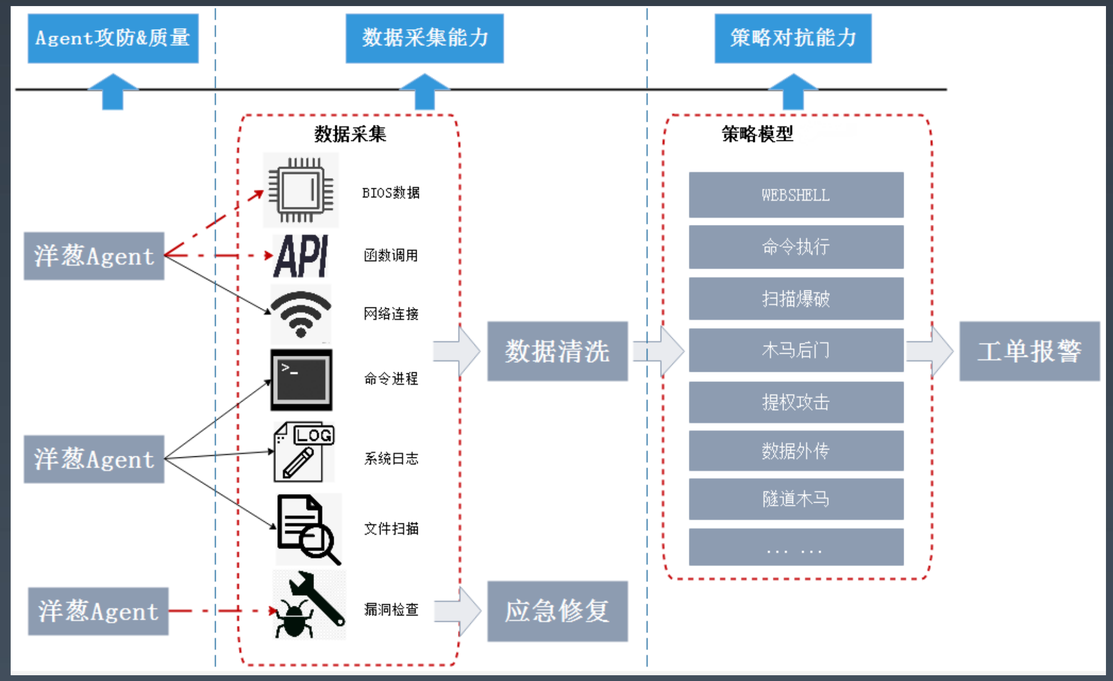
腾讯某服务redis端口对外未鉴权，被植入木马



所有的入侵动作，背后都能看到一条完整的行为链路，在链路中的关键环节层层设防，是反入侵的基本。

反入侵洋葱系统

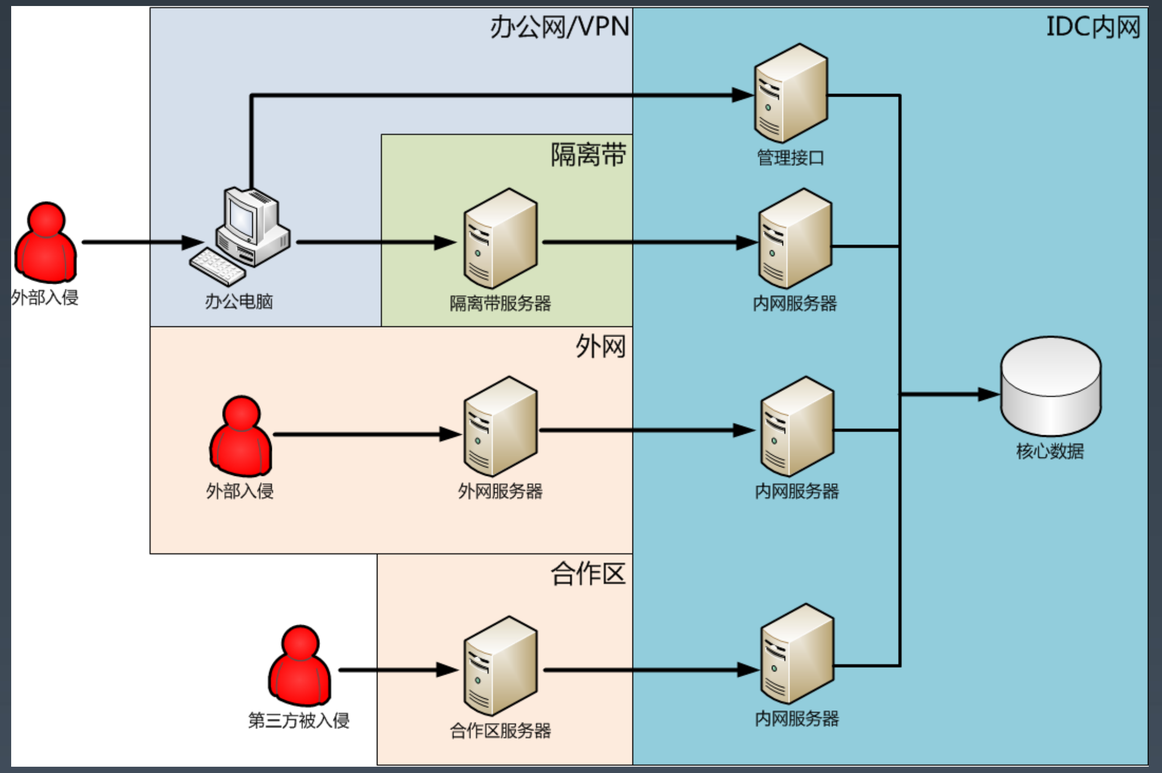
罗卡定律：凡两个物体接触，必会产生转移现象



面临的挑战

- 盘子大：　百万级服务器
- 业务众多：各种应用/第三方软件，自研服务，安全意识
- 网络复杂：生产环境，合作区，腾讯云，隔离带

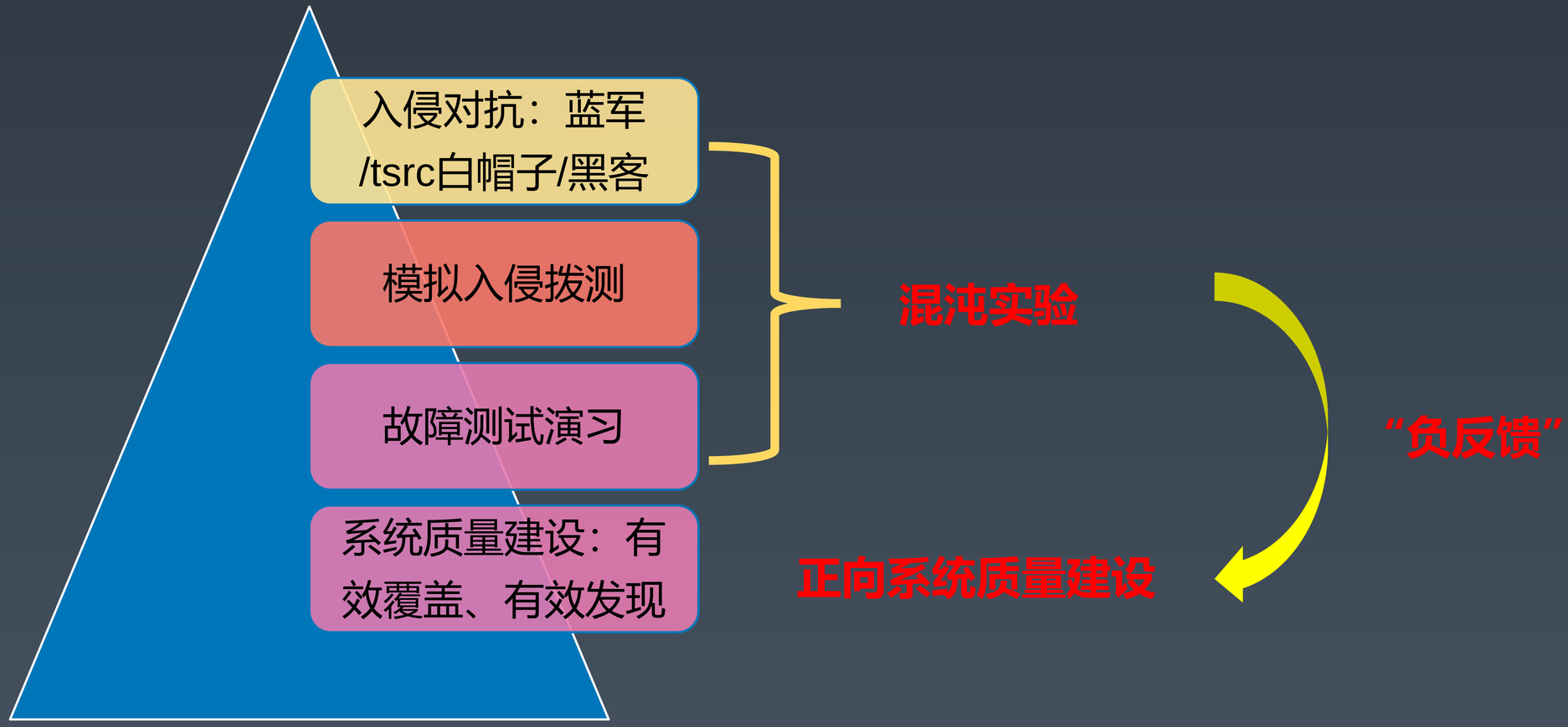
反入侵系统的有效性（质量）至关重要



复杂规模下的质量建设思路

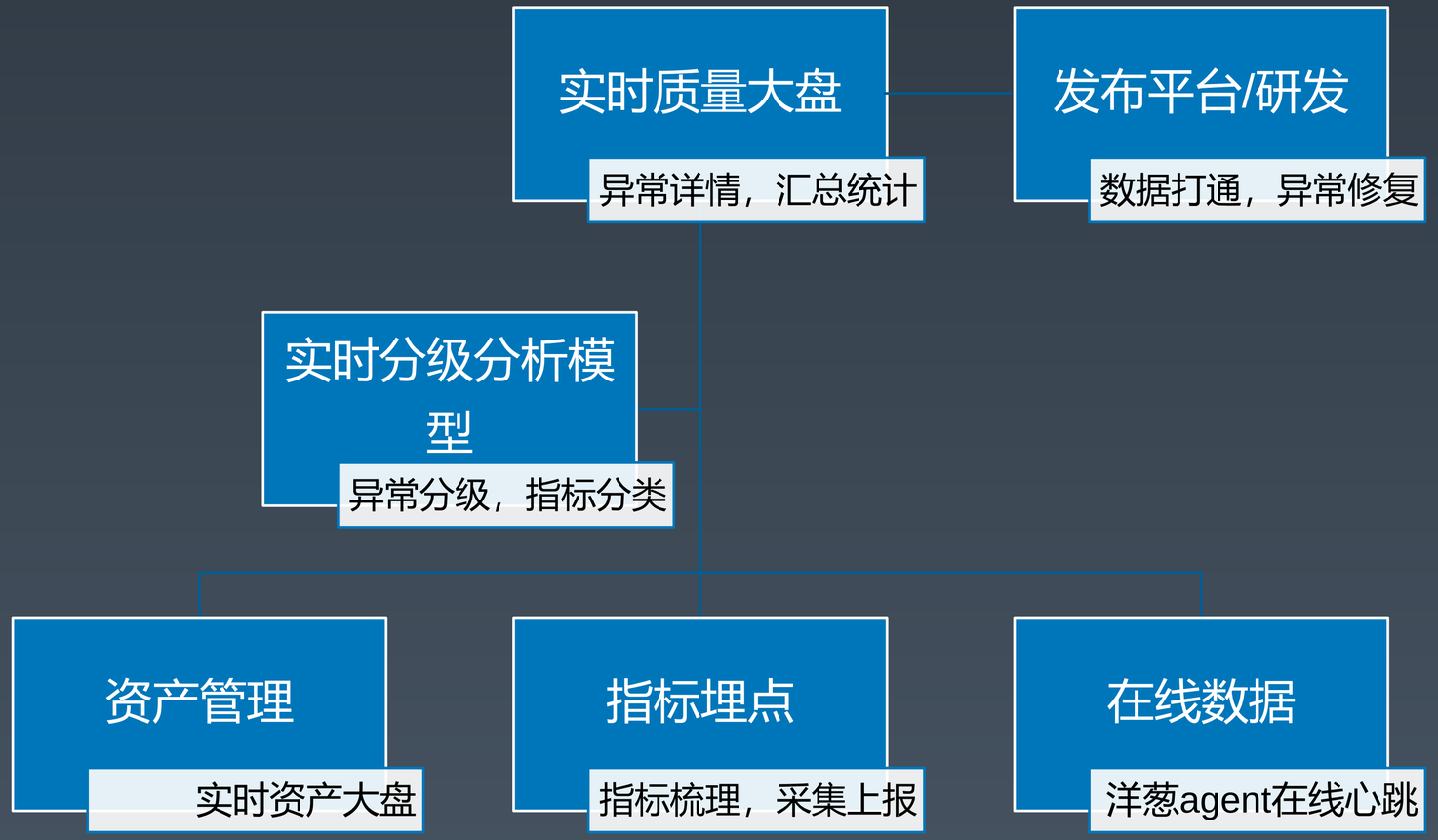
确定能100%覆盖所有异常场景??

复杂规模下的质量建设思路



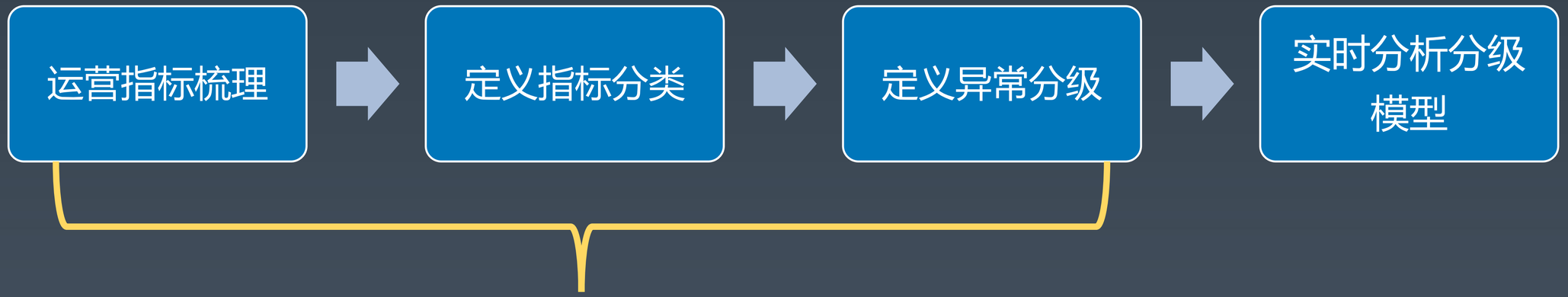
系统质量建设 -- 实时质量大盘

实时质量大盘： 用于实时表述整个客户端系统**有效覆盖率**的健康度指标，以及异常分类统计占比输出；

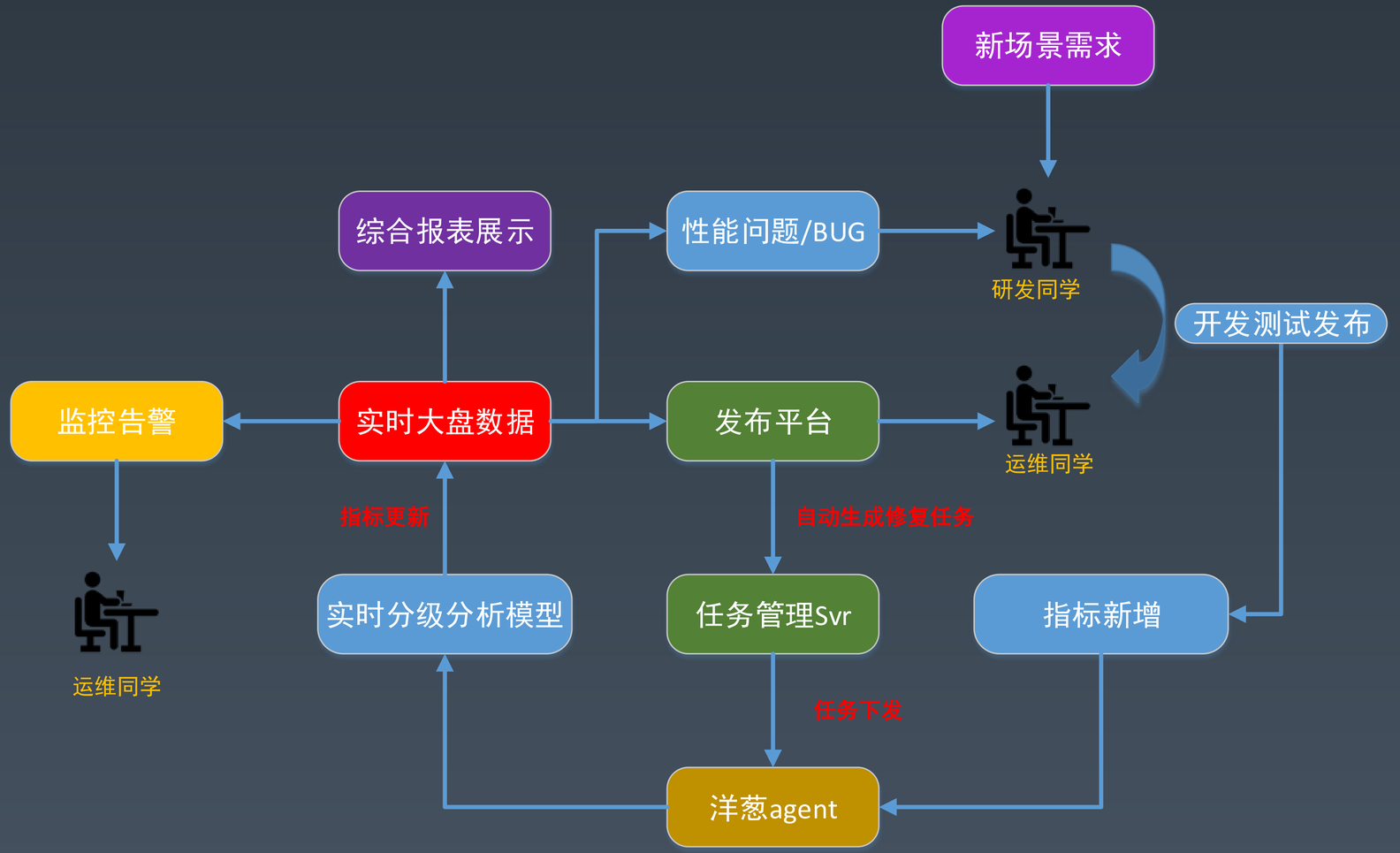


系统质量建设 – 异常分级

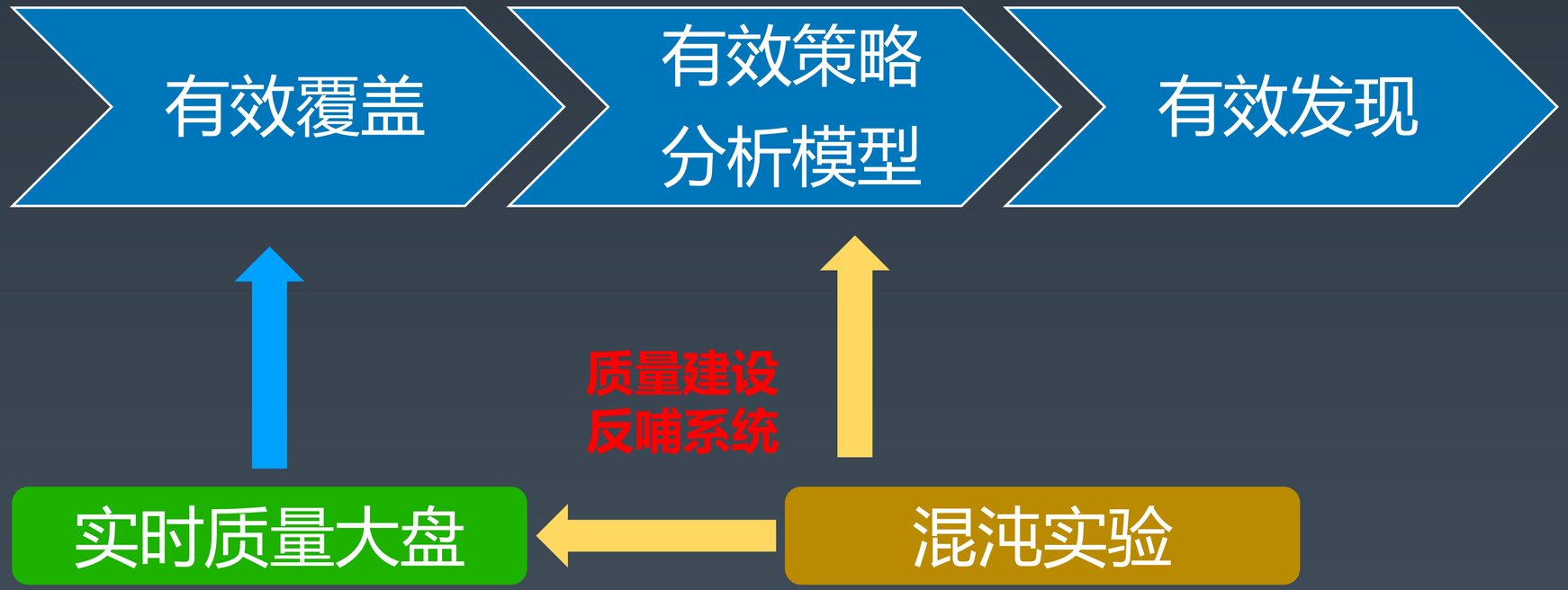
- **分级原则：**区分运维关注和开发关注，影响严重程度
- **分级目的：**指标聚合，突出高风险性异常；运维关注部分，可直接打通发布平台自动修复



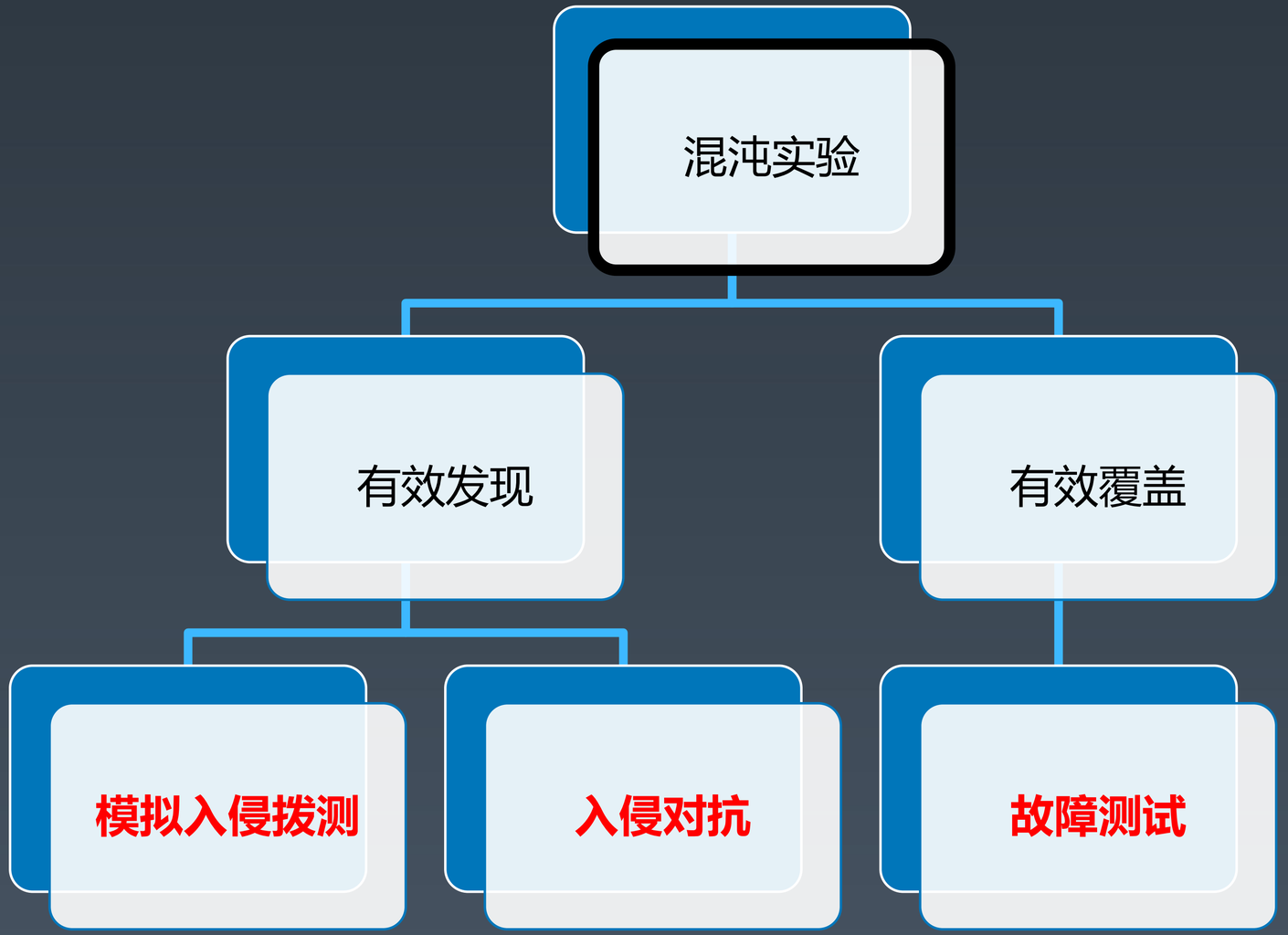
系统质量建设 -- 异常自动修复与输出



混沌实验：反哺系统质量建设



反入侵场景下的混沌实践



反入侵场景下的混沌实践 –故障测试方法

客户端agent	后端接入	分析系统
• 低版本 • 插件未部署 • 接入切换	• 机器高负载 • 主机故障	• 进程退出 • 主机故障

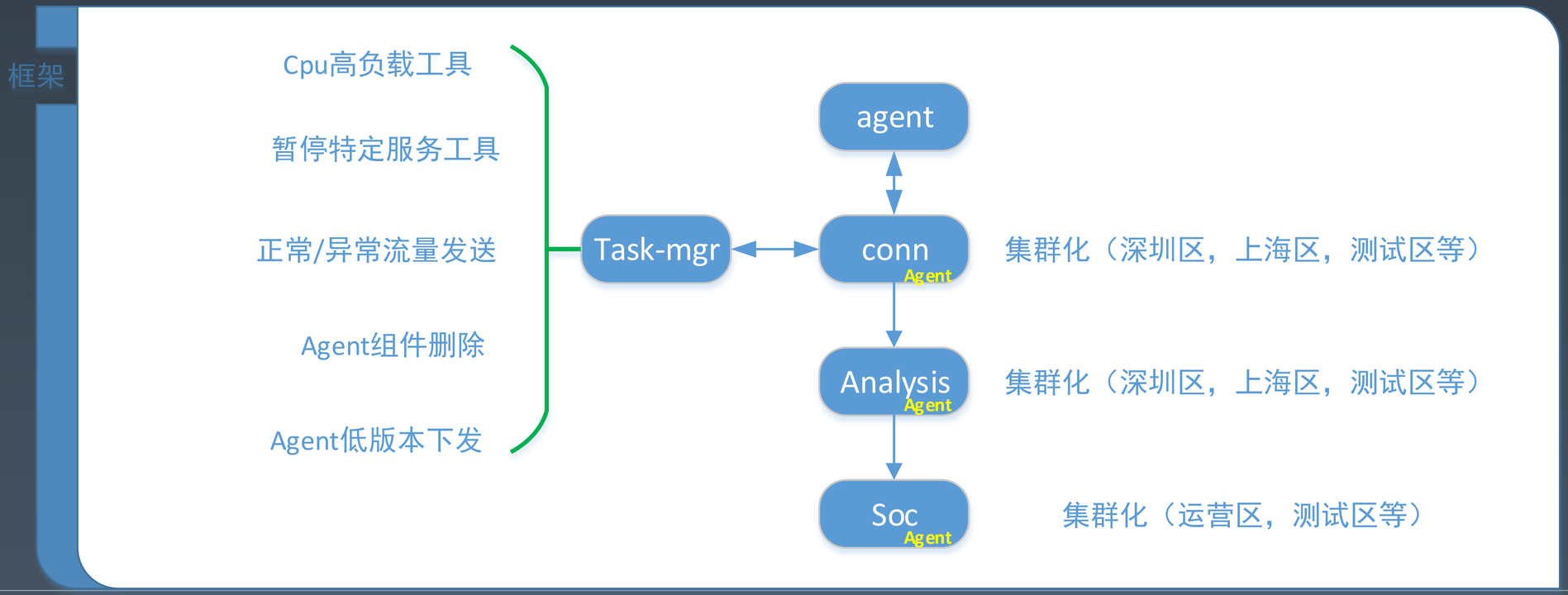
雪崩演练

反入侵场景下的混沌实践 –故障测试方法

所有的服务器，包括业务服务器，和洋葱系统后台服务器，都安装有洋葱agent

反入侵洋葱系统，设计有任务服务，可以向任意agent下发任务执行；

通过任务通道，可以下发任何特定引入故障的工具并执行，从而达到故障注入的效果；

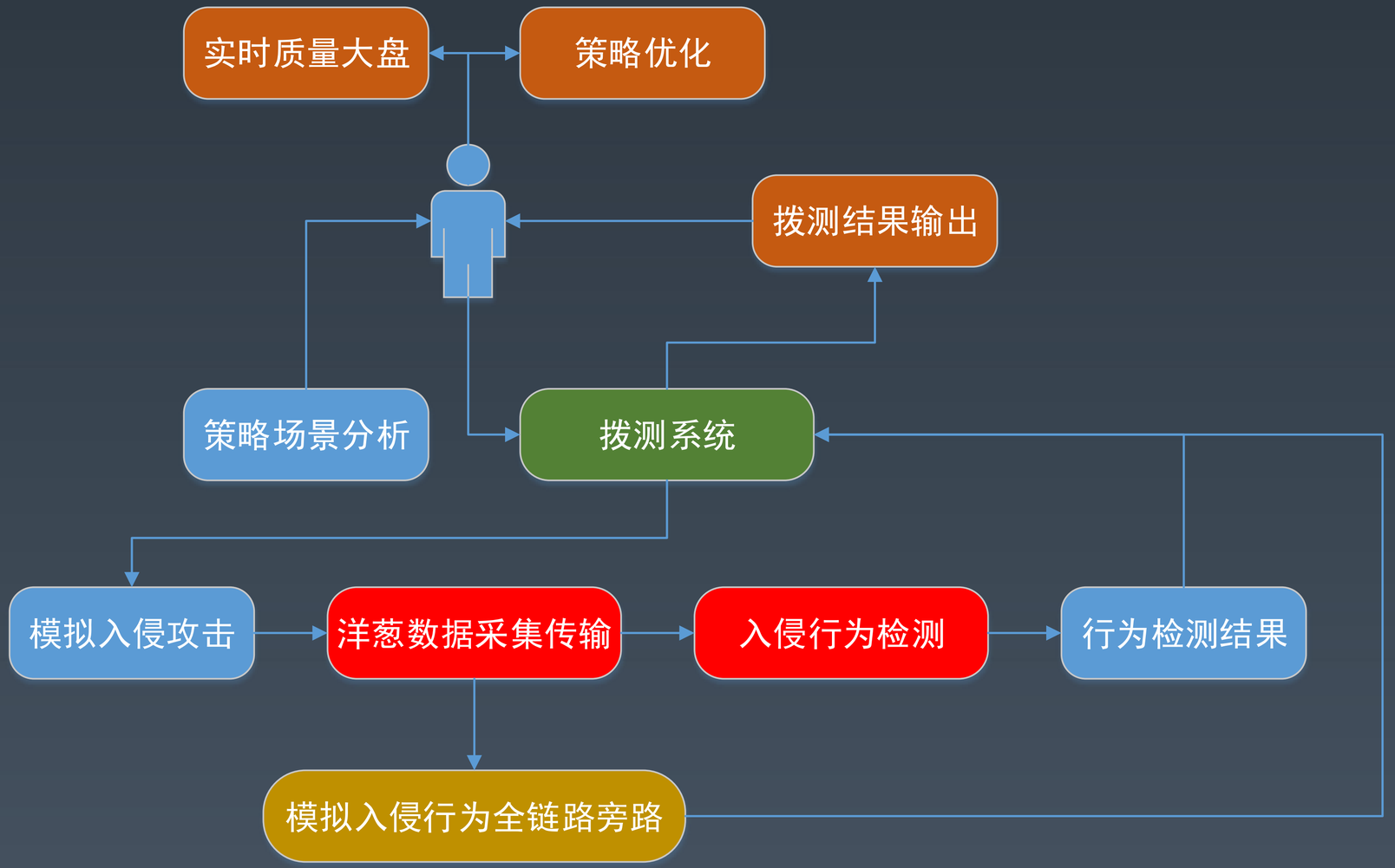


反入侵场景下的混沌实践 – 模拟入侵

- 模拟入侵拨测，是混沌实验在安全场景下，旨在**策略场景反向验证**，和反入侵系统质量验证的一种实验方法。

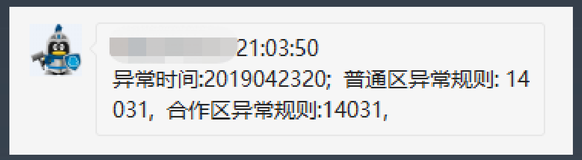
- 模拟入侵拨测，具备以特征：
  1、覆盖所有现网提供服务的策略场景
  2、黑盒实验，周期性触发，自动化验证测试结果
  3、拨测数据全链路日志染色落地

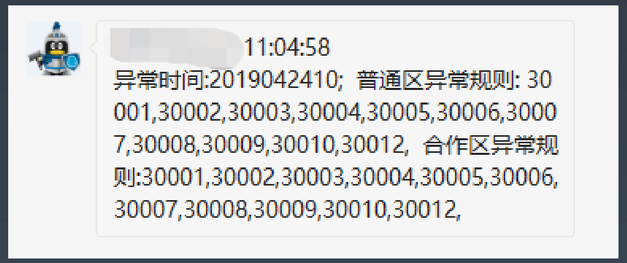
模拟入侵拨测


实时质量大盘
策略优化
拨测结果输出
策略场景分析
拨测系统
模拟入侵攻击
洋葱数据采集传输
入侵行为检测
行为检测结果
模拟入侵行为全链路旁路

模拟入侵拨测

效果与作用： 历史上发现现网环境中，多起**测试监控未覆盖场景下**，策略和质量问题（发布前未知），挖出了不少引起异常波动的**隐患因素**





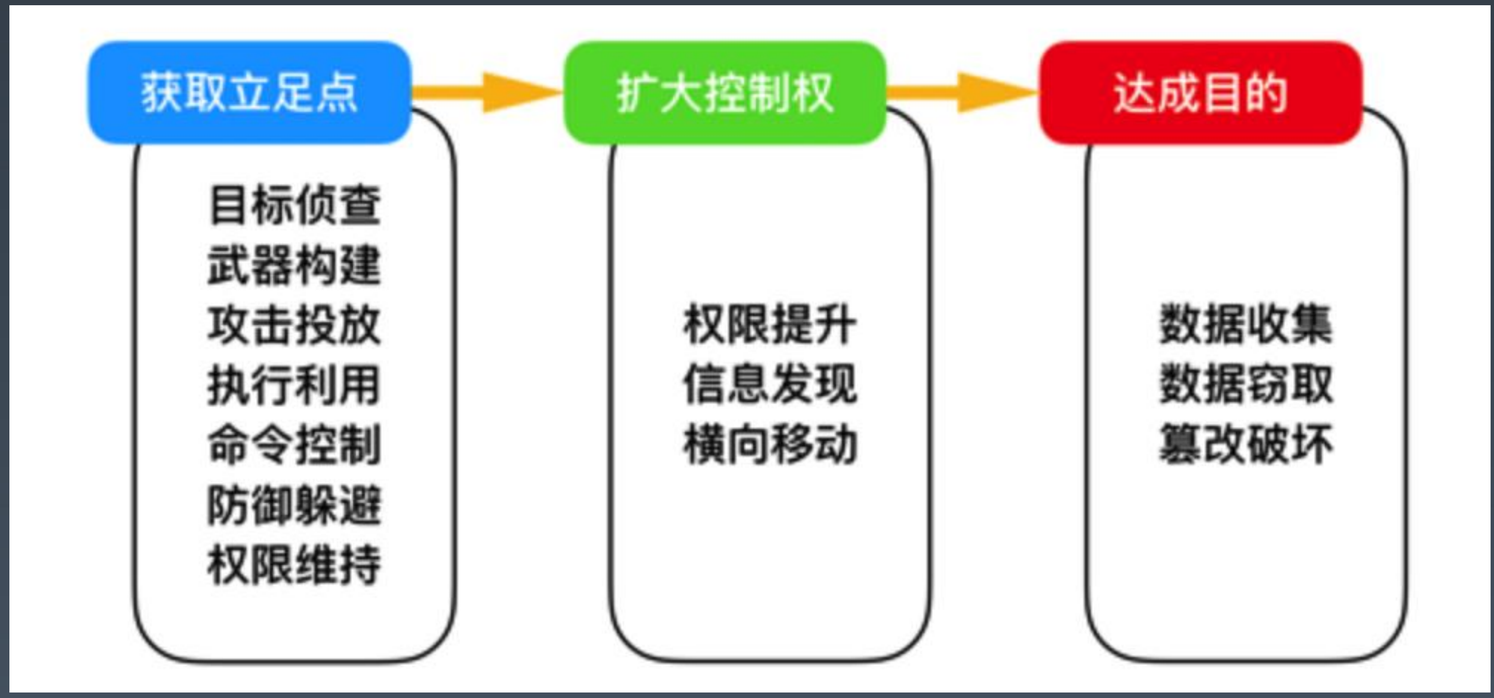
入侵对抗

- 入侵对抗，是混沌实验在安全场景下的一种实验方法，实验对整个安全系统的入侵有效发现进行验证，，**目的是检验在真实攻击中纵深防御能力、告警运营质量、应急处置能力**，以此发现系统入侵数据采集、策略建设中的薄弱点和漏水，然后推动系统完善和改进。

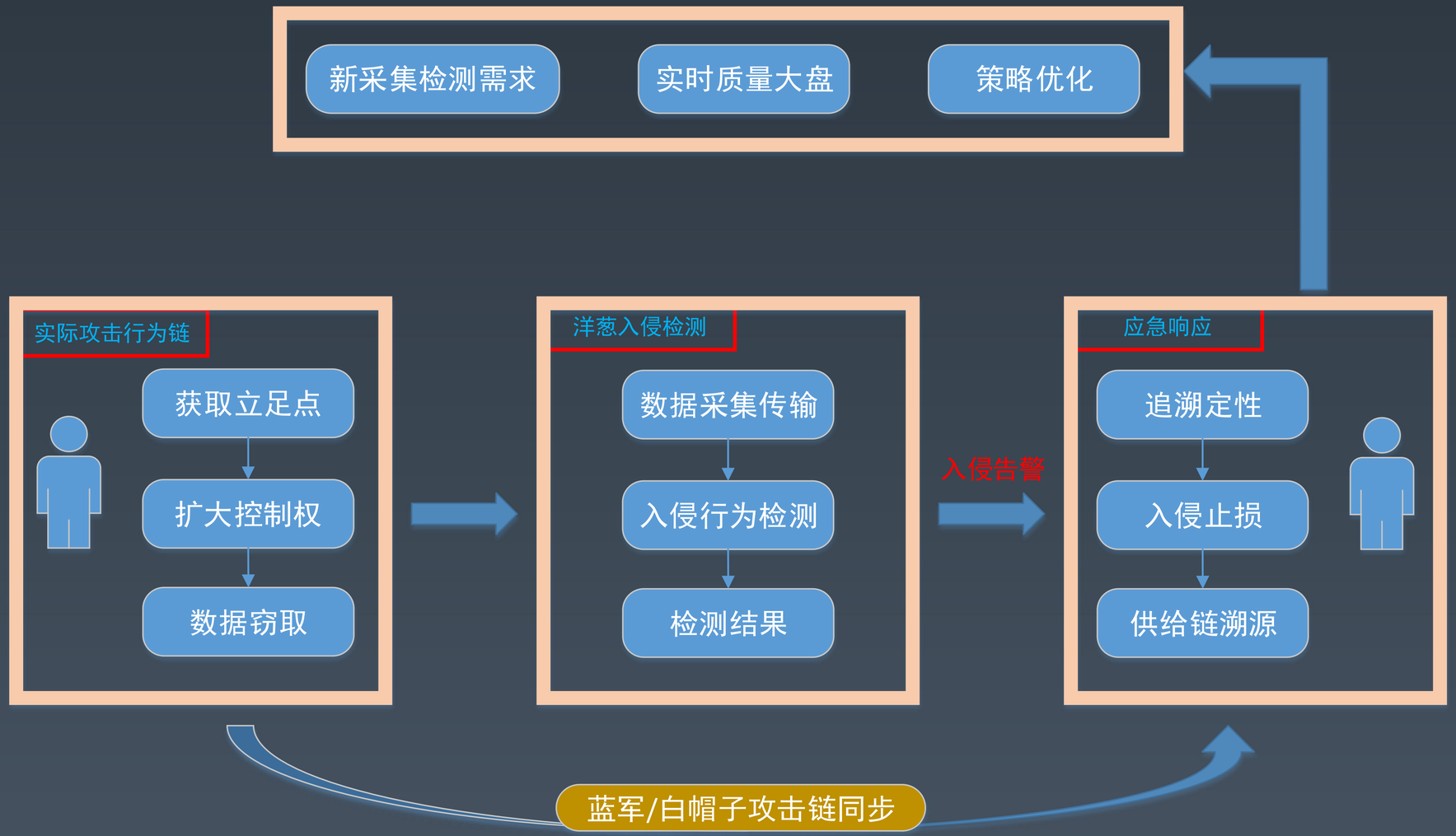
- 入侵对抗实验，主要分下面两个角度：
  1、**内部蓝军演习**对抗（类似实际入侵，非策略验证）；
  2、tsrc（**白帽子**）/**实际入侵**

入侵对抗：蓝军/白帽子/黑客

以获取服务器或数据控制权限为目标的完整攻击演习，或者实际入侵行为；

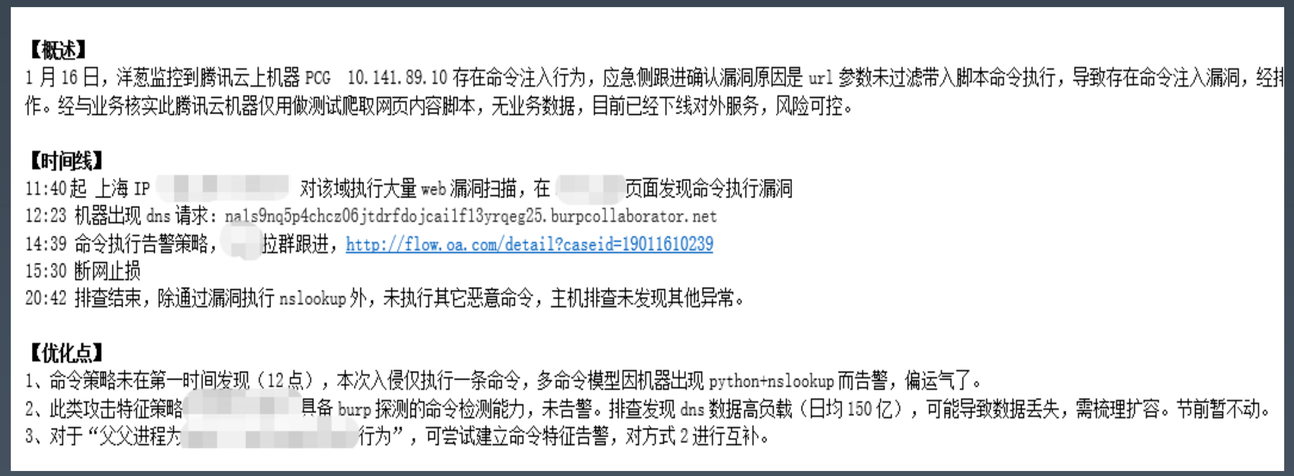


入侵对抗闭环


新采集检测需求
实时质量大盘
策略优化
实际攻击行为链
获取立足点
扩大控制权
数据窃取
洋葱入侵检测
数据采集传输
入侵行为检测
检测结果
入侵告警
应急响应
追溯定性
入侵止损
供给链溯源
蓝军/白帽子攻击链同步

入侵对抗闭环

- 完整验证入侵检测全流程有效性
- 每次漏水或异常，都能给入侵发现带来新的场景知识和补充
- 有效发现系统薄弱点和隐患，并能推动短板补齐



总结与展望

➢ 总结回顾

本次介绍了反入侵相关的背景，以及反入侵洋葱系统在质量建设方面的思路和推进方法。从反入侵场景下质量建设的出发，看待分布式系统的质量建设，需要从正反两个方向入手，动态互补，才能不停推进系统的稳定和有效；

1）**正向质量建设**：解决可预知的可能出现异常的监控和优化，沉淀了复杂系统规模下实时质量大盘建设的思路和方法

2）**反向质量建设**：通过混沌实验，从系统的目标场景触发，检验在故障，或者现实非预知情况下，是否能够完整的实现目标，从而形成负反馈，推进正向质量建设。沉淀了一整套模拟入侵检验的自动化系统，以及实际入侵对抗下的质量闭环系统

➢ 未来规划

1） 将细化，自动化故障注入验证引入现网运营环境，演习常规化；

2） iot智能硬件，服务器底层（BIOS等）更高层次对抗能力和质量建设

极客时间 | 企业服务

这是一封正经“福利”贴

想做团队的领跑者 需要迈过这些“槛”

成长型企业，易忽视人才体系化培养 企业转型加快，团队能力又跟不上	VS	从基础到进阶，超100+一线实战 技术专家带你系统化学习成长
团队成员技能水平不一， 难以一“敌”百人需求	VS	解决从小白到资深技术人所遇到 80%的问题
寻求外部培训，奈何价更高且 集中式学习	VS	多样、灵活的学习方式，包括 音频、图文 和视频
学习效果难以统计，产生不良循环	VS	获取员工学习报告，查看学习 进度，形成闭环

课程顾问「橘子」

回复「QCon」
免费获取
学习解决方案

 # 极客时间企业账号 # 解决技术人成长路上的学习问题

GTLC
GLOBAL
TECH LEADERSHIP
CONFERENCE
全球技术领导力峰会

Geekbang. 极客邦科技 | TGO 鲲鹏會

500+高端科技领导者与你一起探讨
技术、管理与商业那些事儿

2019年6月14–15日 | 上海圣诺亚皇冠假日酒店

扫码了解更多信息

THANKS!

QCon 10th