



# 网络安全运营的几点体会

黄眉

阿里巴巴本地生活风控与安全中心负责人

网络安全运维 是 职能；网络安全运营 是 业务，为逆向型的安全业务结果负责

今天，我们处于网络安全运维向网络安全运营过渡的阶段



- 被动响应
- 缺乏沉淀
- 杂乱无章

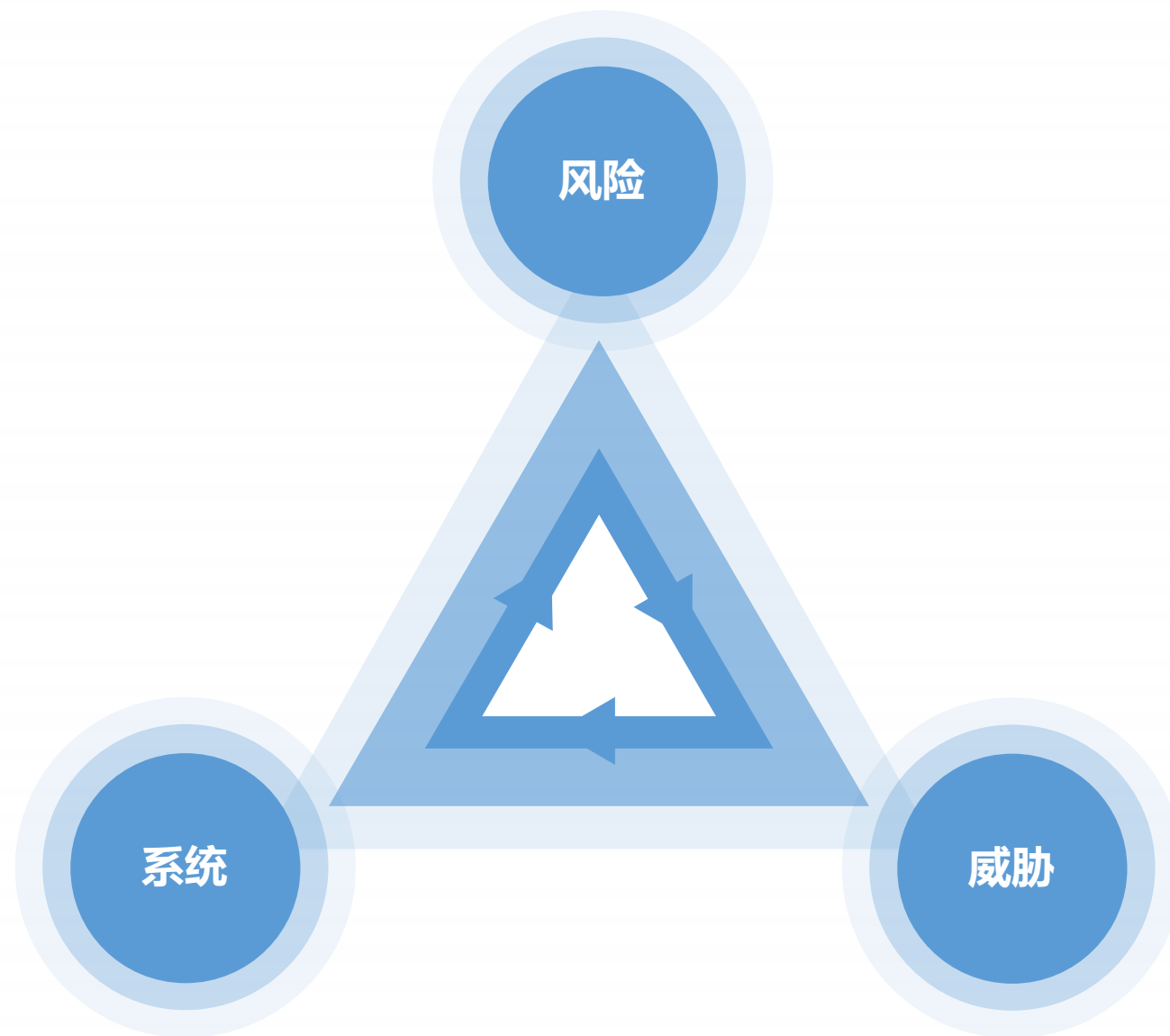


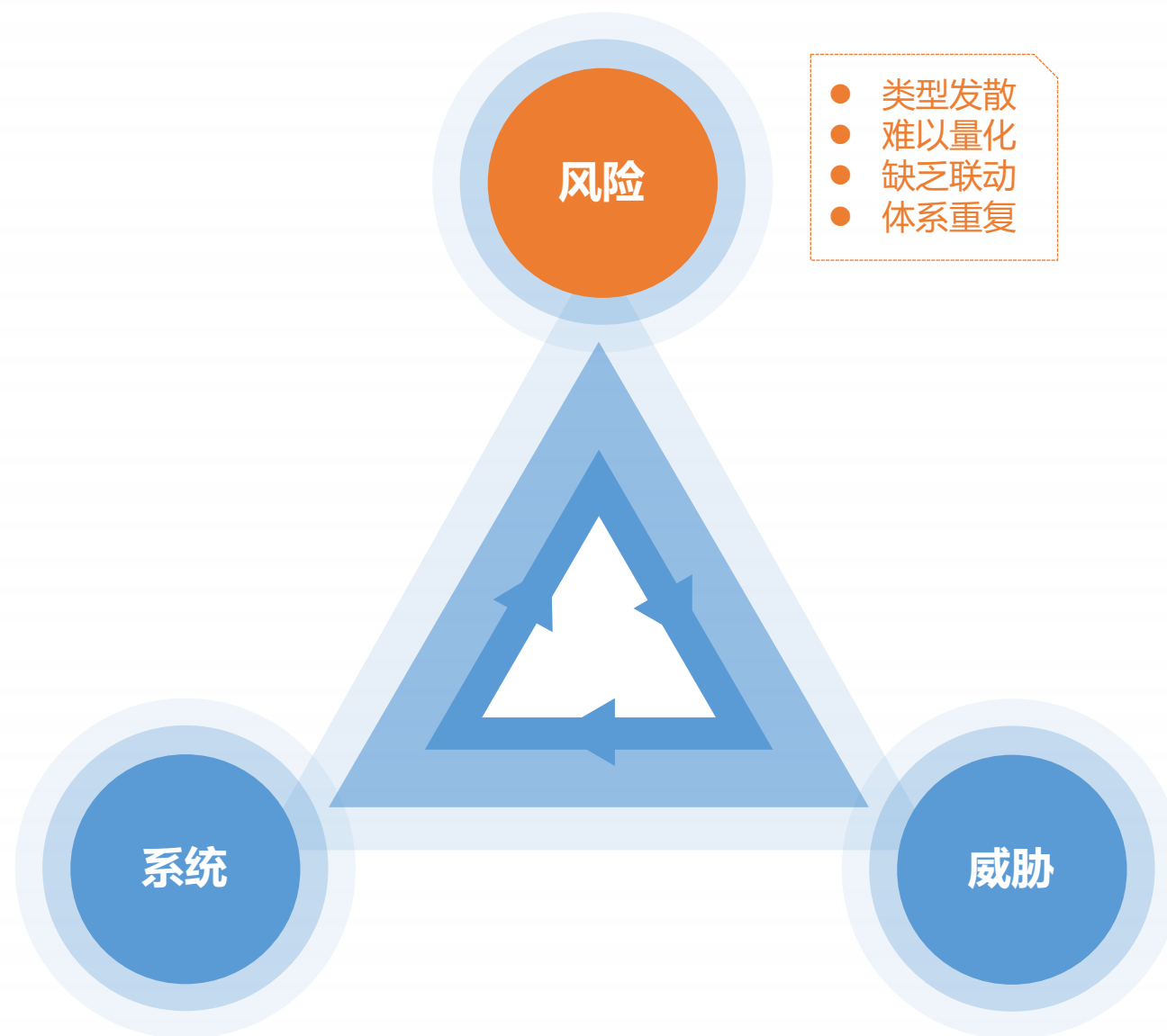
- 主动布局
- 增长思维
- 形成体系

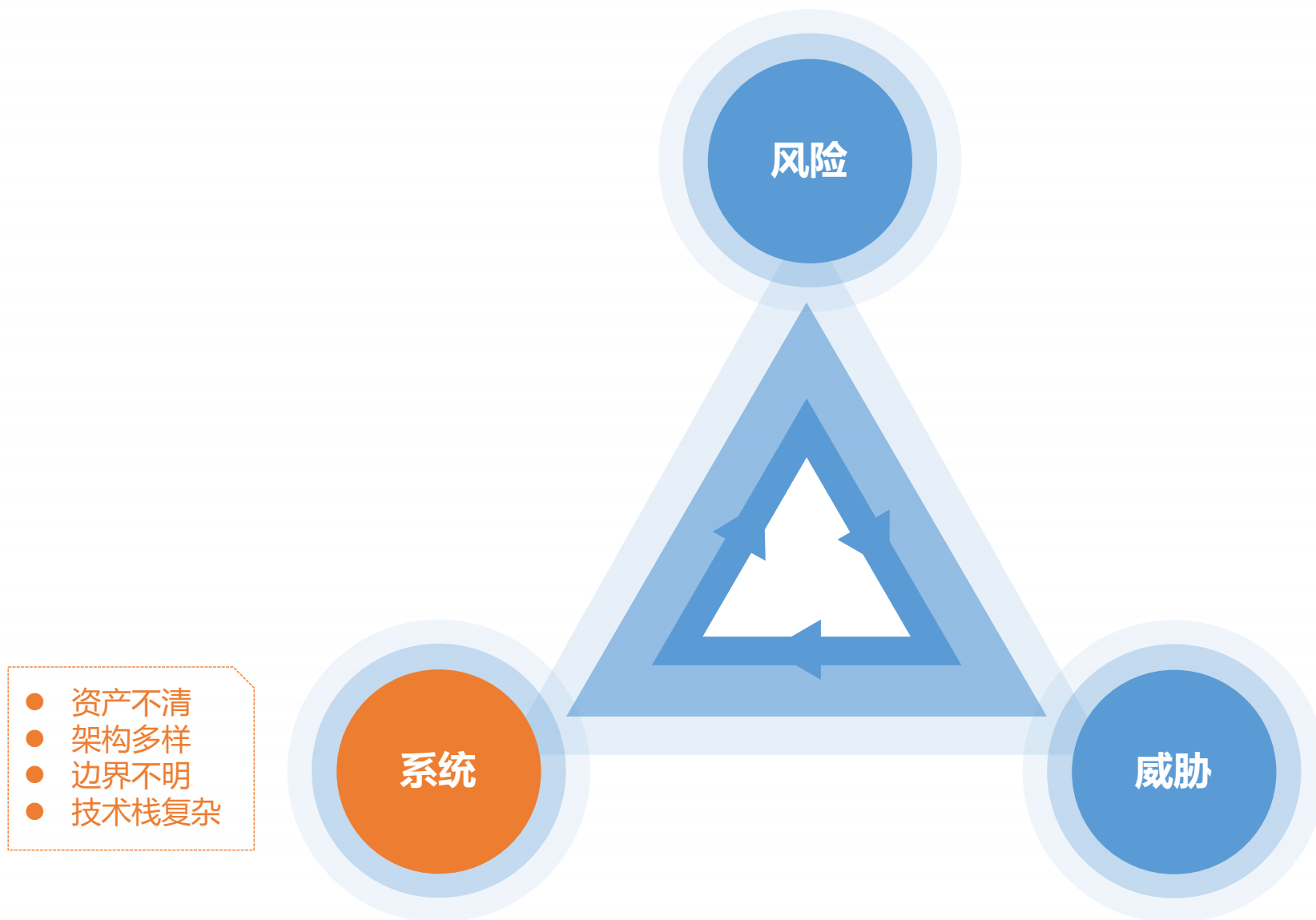


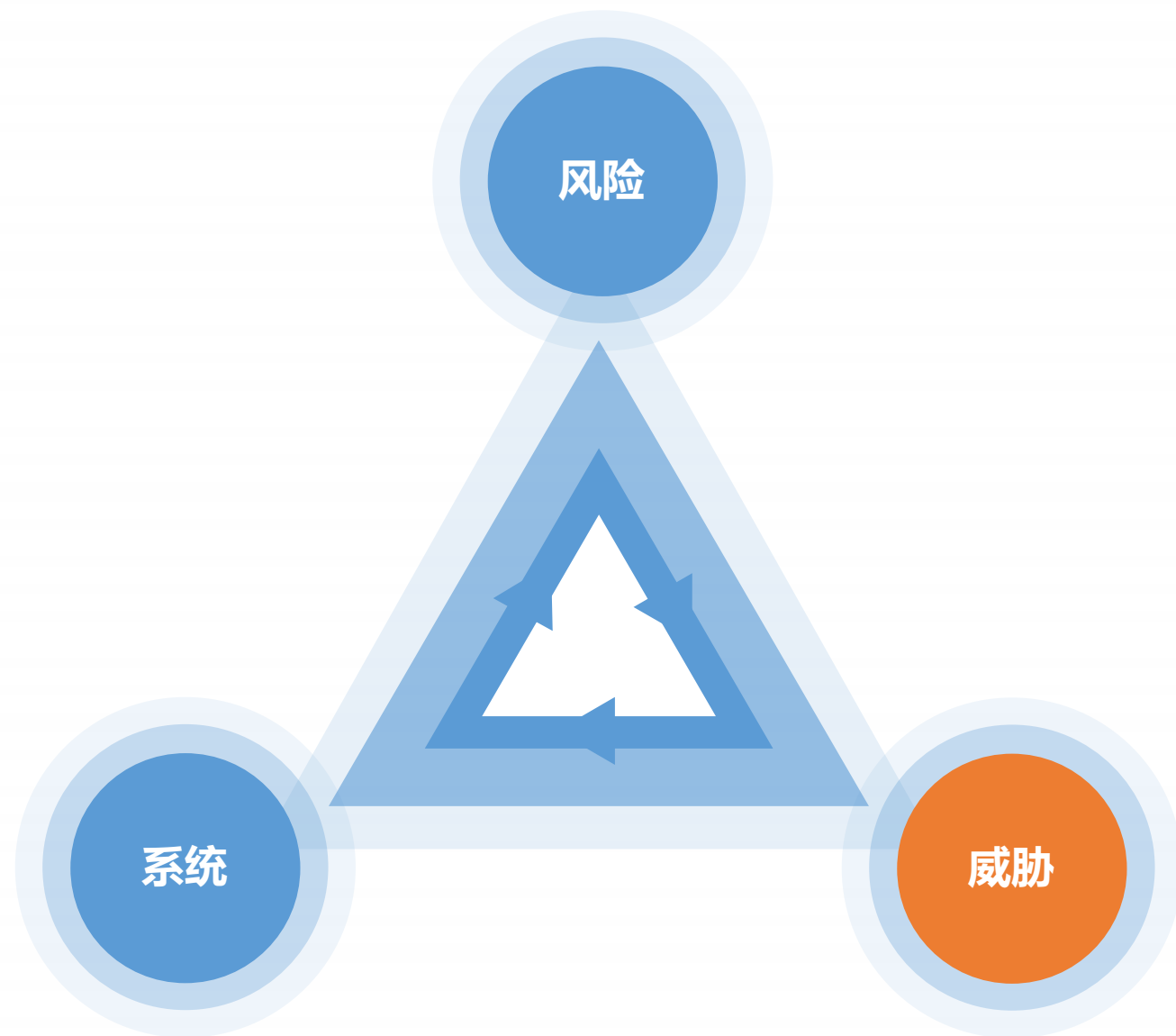
- 改变业务
- 塑造基因
- 形成共识







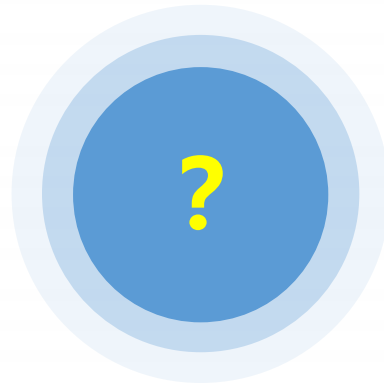




- 看不见
- 看不清
- 来不及

# 如何解决？

2019 北京网络安全大会  
2019 BEIJING CYBER SECURITY CONFERENCE



- 双十一有很多风险
- 其中稳定性风险，特别是11.11零点高峰的性能容量稳定性风险是超级挑战的
- 这个稳定性和安全的关系及其密切（DDoS攻击、CC攻击、大规模垃圾流量、业务系统超载等等）
- 要解决这个风险，需要一整套的体系

## 威胁

DDoS  
团伙

黑客攻  
击者

羊毛党

其他群  
体

## 双十一头15分钟稳定性风险

技术/业务故障

DDoS攻击

CC攻击

黄牛党机器流量

DoS 0day

## 系统

千万QPS/核心网关

百万服务器

万级应用/100+app

千次变更/周

近百个BU

全链路攻防





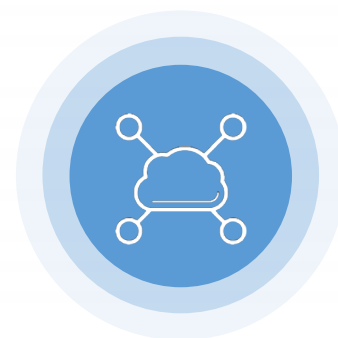
反入侵



数据防泄漏



反爬



反作弊



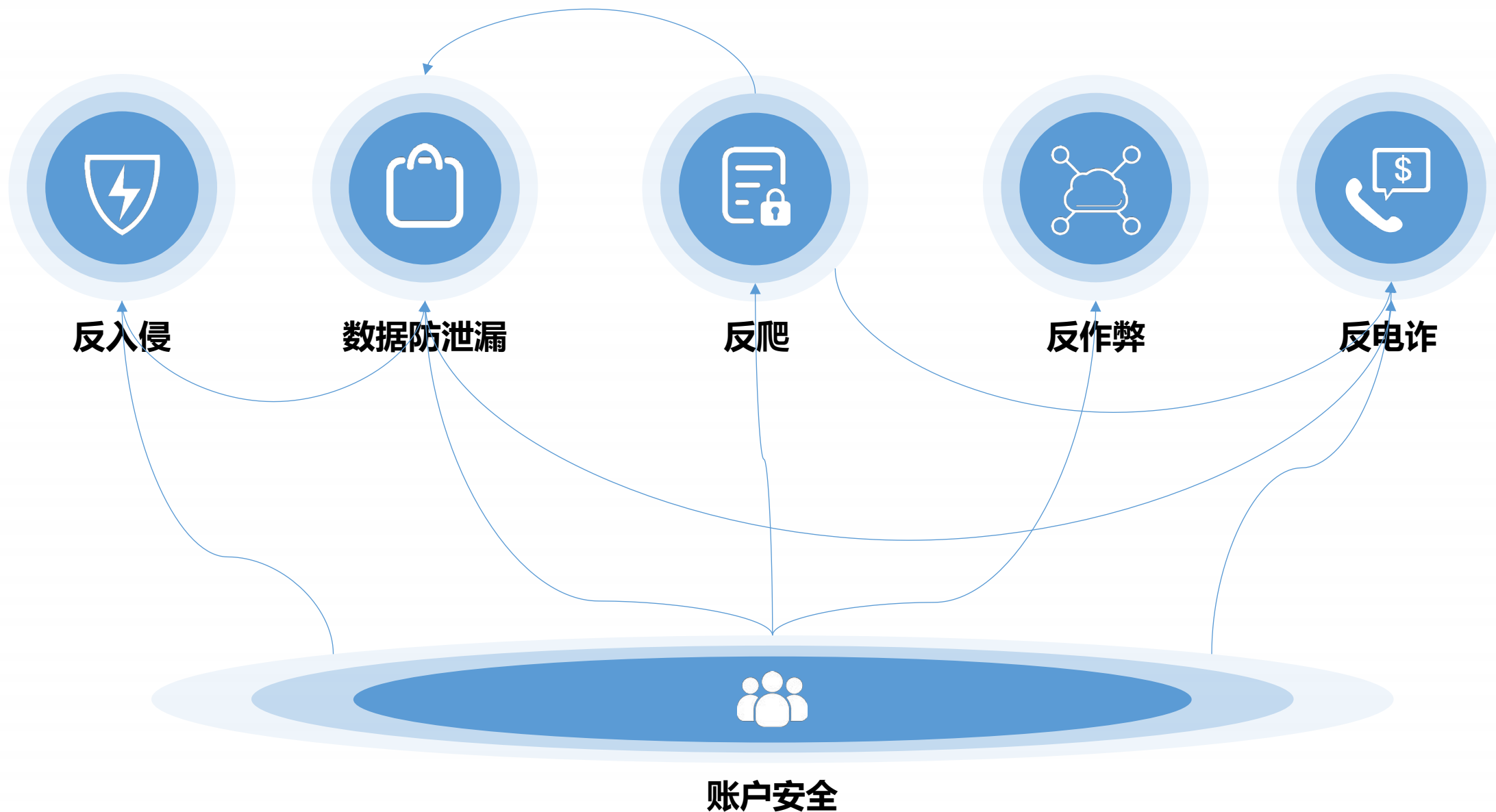
反电诈



账户安全

# 这些风险场景有何关系？

2019 北京网络安全大会  
2019 BEIJING CYBER SECURITY CONFERENCE



# 这些风险场景有何不同？

2019 北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE



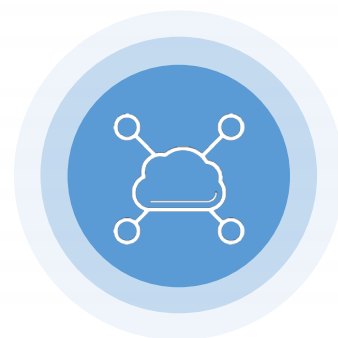
反入侵



数据防泄漏



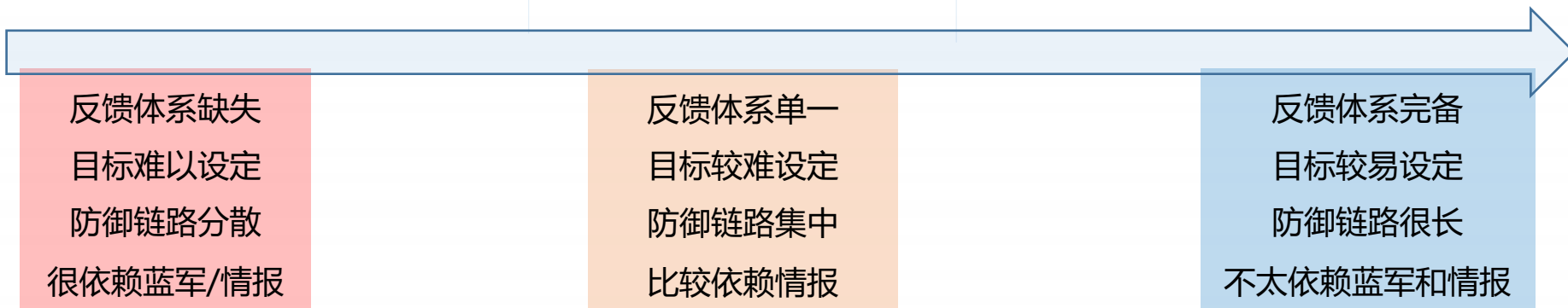
反爬



反作弊



反电诈

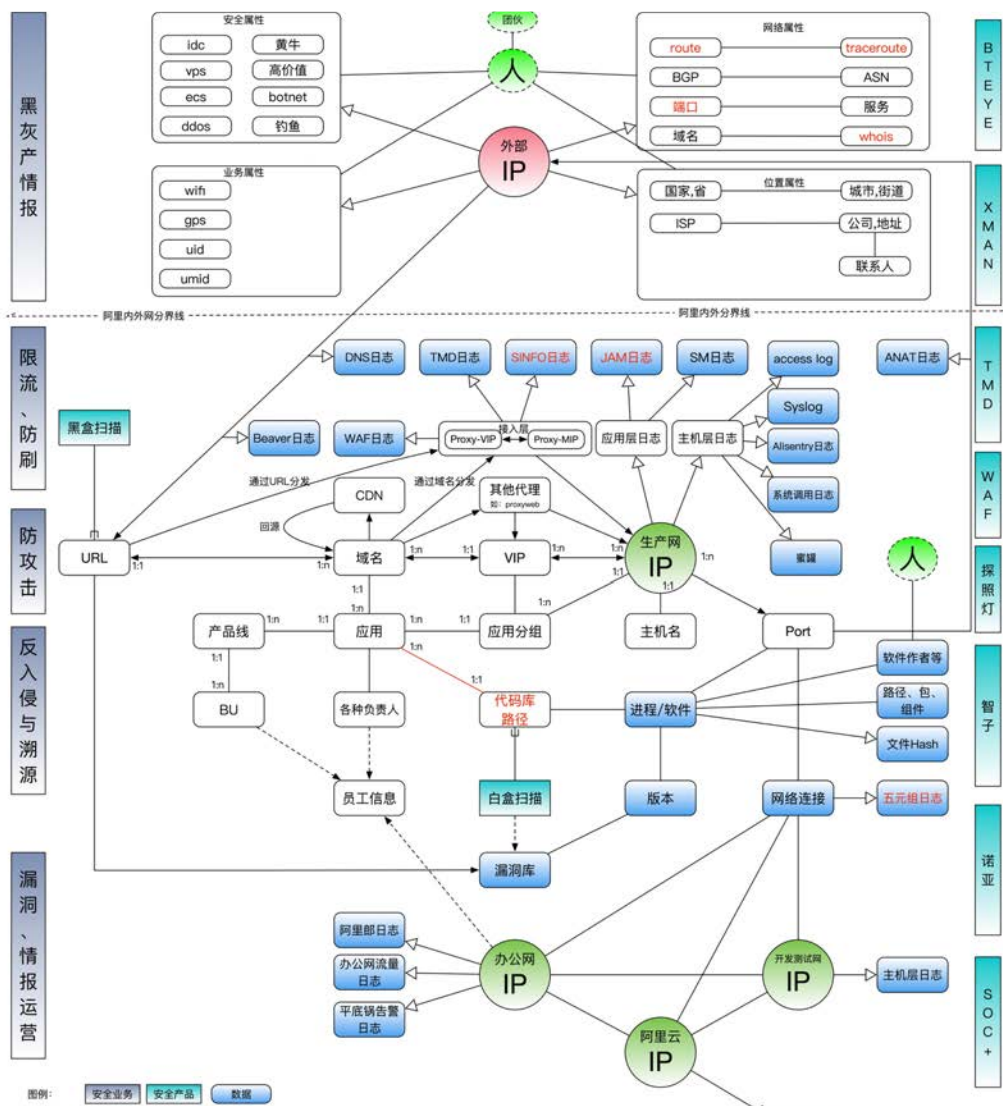


账户安全

风险归类 + 风险分层 + 风险联动 = 风险网络




- 通过架构归约逐步降低系统复杂度
- 良好的架构是系统数据化的基础(ROI)
- 数清楚自己有什么、是核心竞争力
- 通过数据刻画系统之间的关系
- 通过数据刻画数据流动
- 通过内生数据挖掘情报



- 乙方的威胁情报+甲方的安全架构良好的系统+架构逐步归一化的风控体系+风险网络
- 安全技术+业务的中台在超大平台会逐步成型
- 未来安全行业的“双十一”总有一天会成为现实



The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that form a grid or mesh-like structure, creating a sense of depth and movement.

# THANKS

**2019北京网络安全大会**

2019 BEIJING CYBER SECURITY CONFERENCE