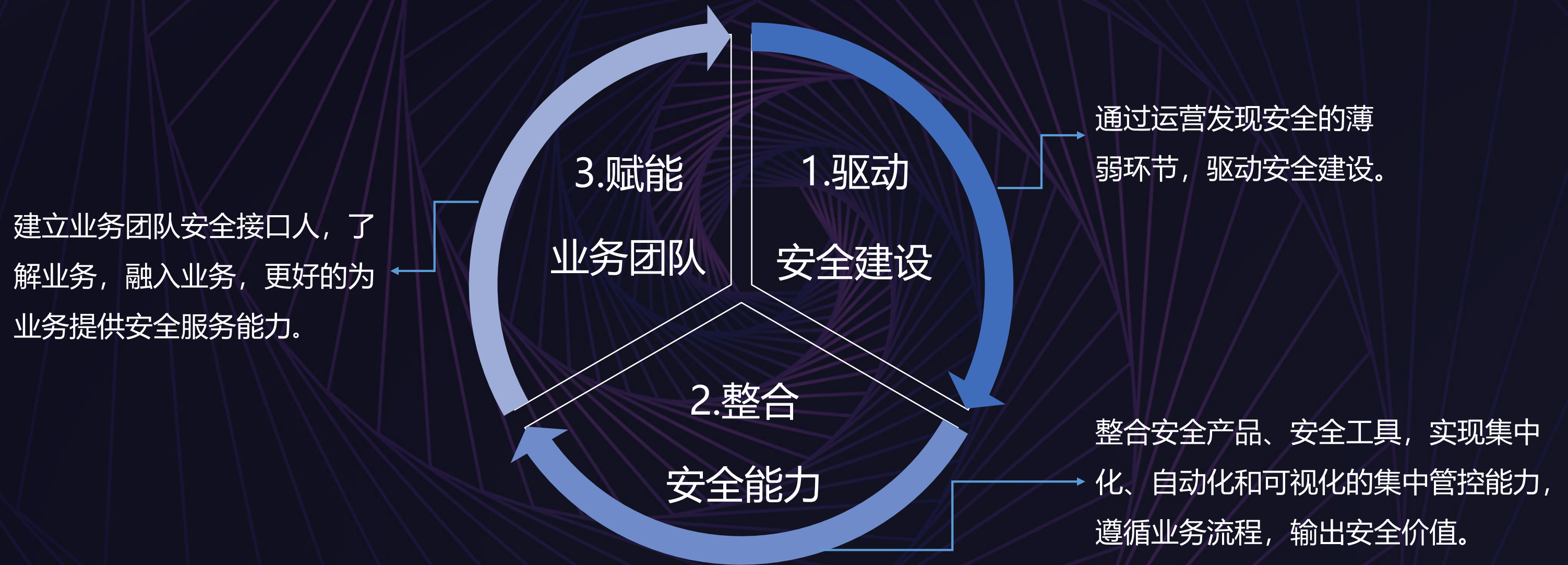


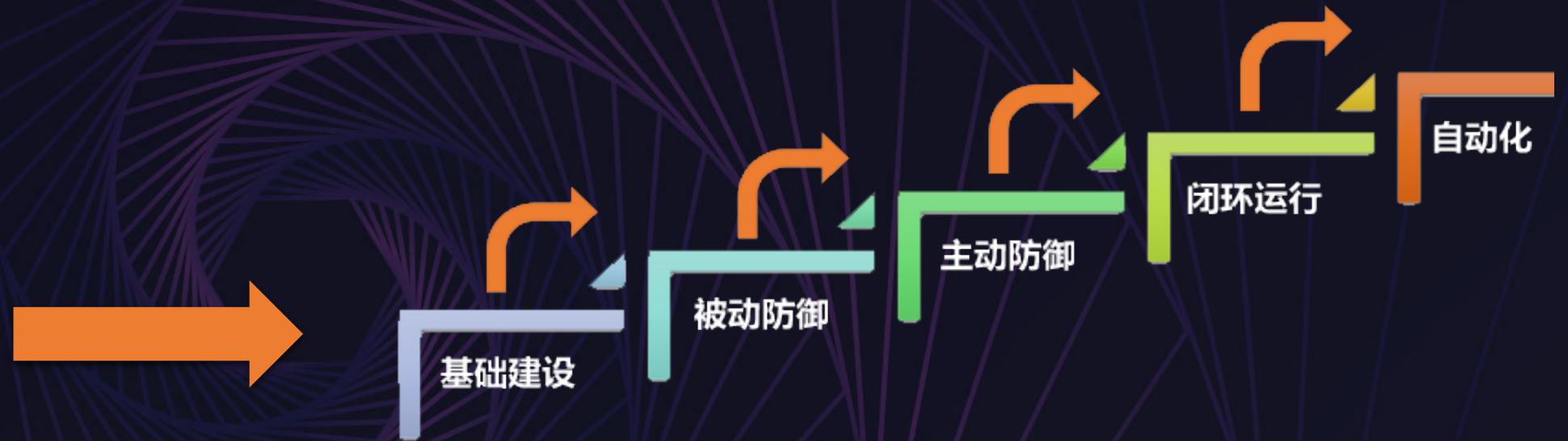
捍 卫 信 任 2 0 1 9 京 麒 国 际 安 全 峰 会

车好多安全运营实践

为什么要做安全运营



安全运营遵循的框架和方法



CYBERSECURITY FRAMEWORK

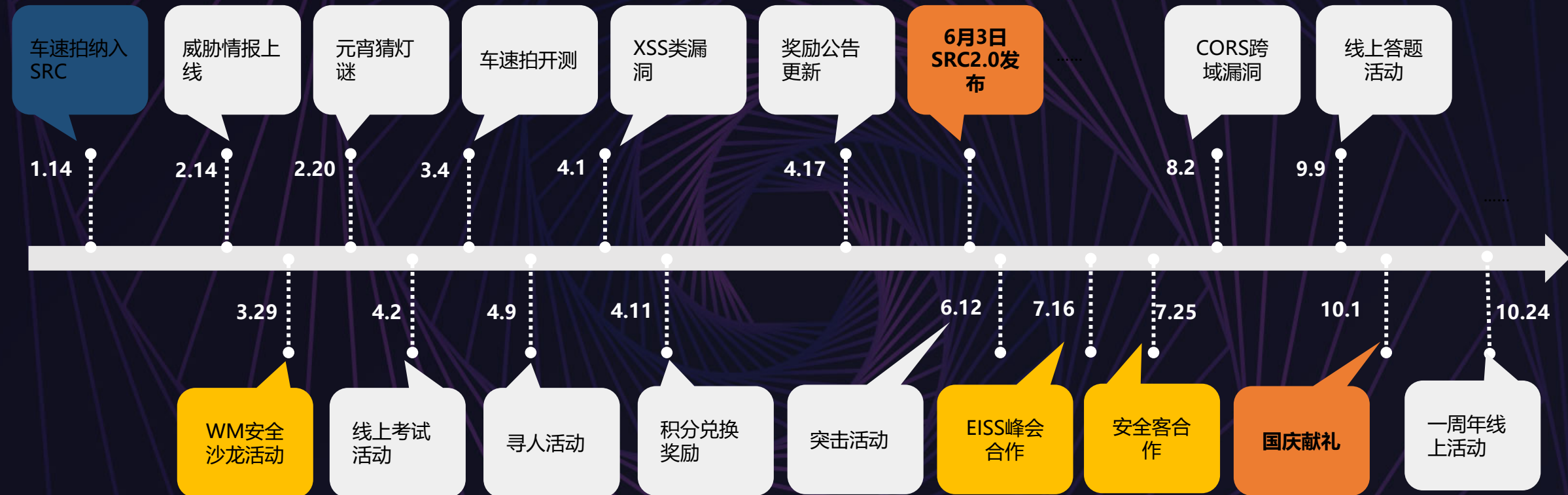
通过在识别、保护、检测、反馈和恢复环节不断优化，最终持续提升整体企业整体安全水平。

安全运营的内容

安全运营的内容



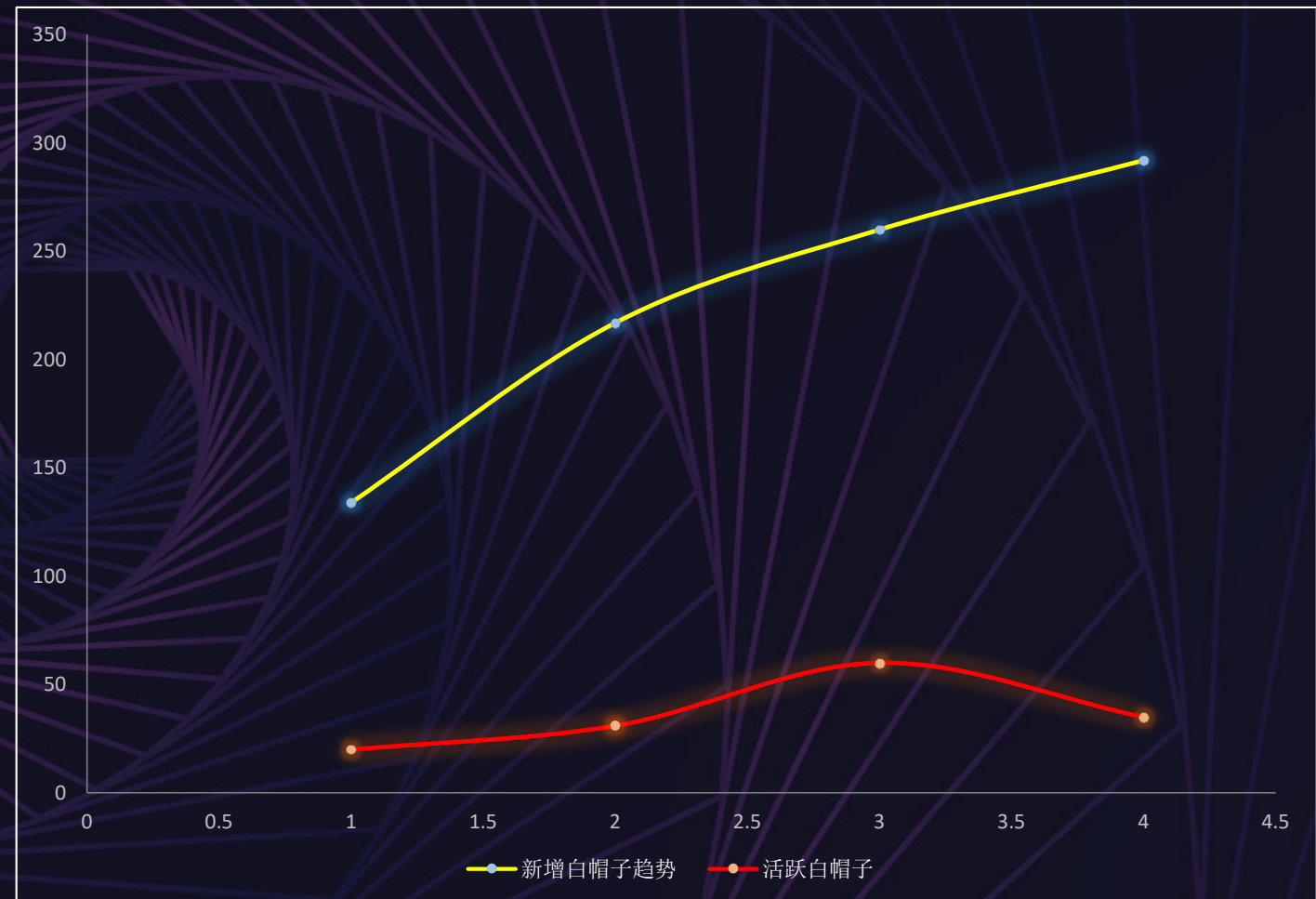
SRC活动运营



- 提升影响，畅通渠道，降低不可控风险因素，通过组织活动GZSRC在白帽子圈的影响力和口碑进一步增加。

SRC用户运营

类别	Q1	Q2	Q3	Q4
新增白帽子趋势	134	217	260	292
活跃白帽子	20	31	60	35



SRC品牌运营

渠道合作

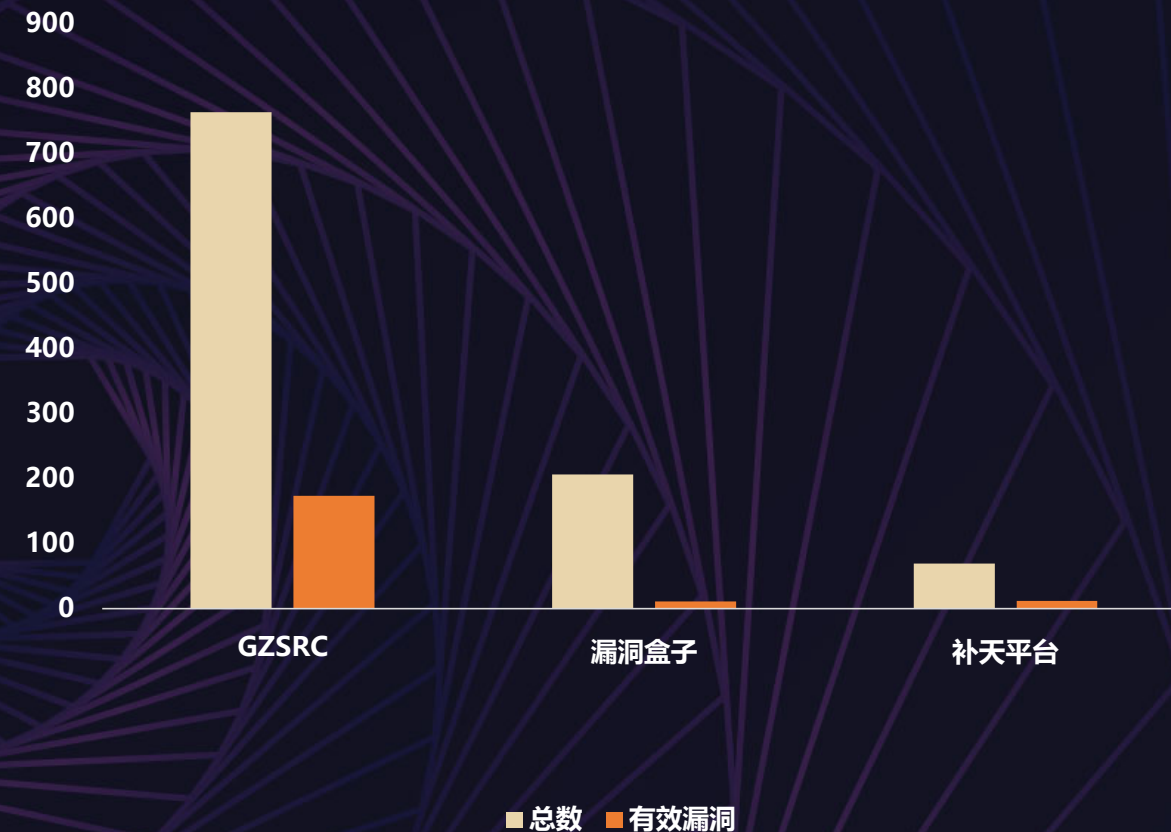


• 互动：25家SRC



品牌影响

GZSRC运营成果



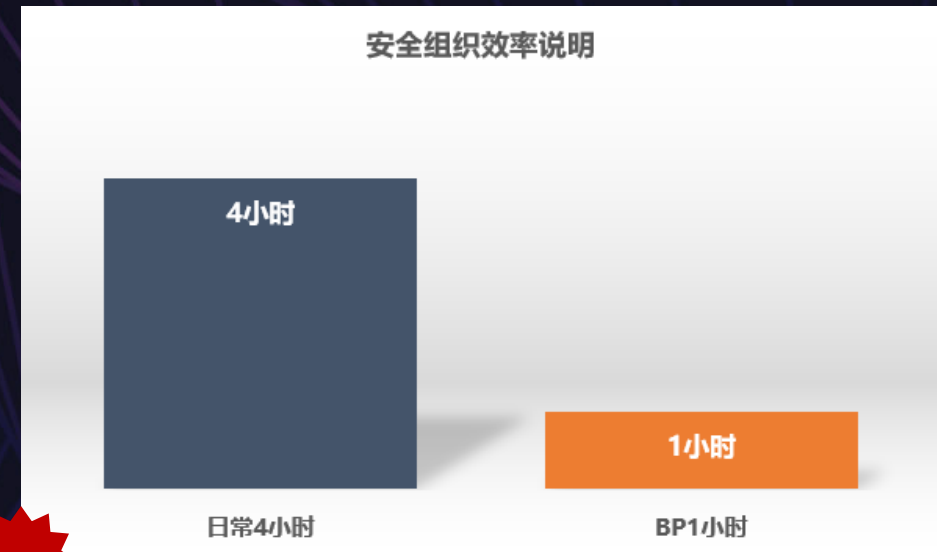
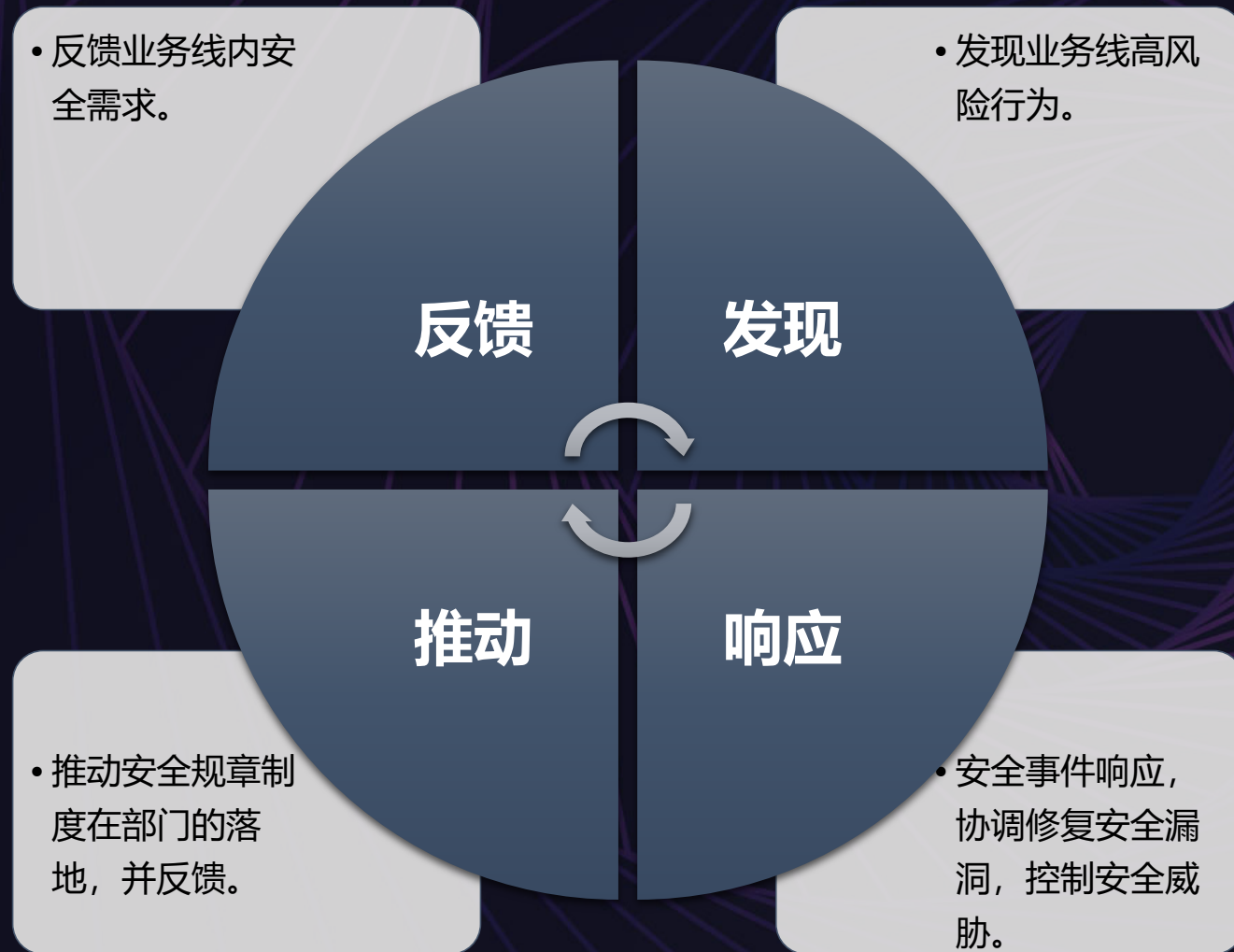
- 通过安全运营, GZSRC有效收集能力大大增强, 随着安全防护手段的完善, 漏洞提交量趋向减少。通过活动运营、用户运营和品牌运营, 大大减少企业因为安全漏洞带来的风险。

运营措施-运营组织建设



- 安全接口人，也称安全BP，是车好多集团安全工作开展的纽带和桥梁。
- 建立高效的沟通反馈渠道、事件发现渠道，也助推SDL等工作的落地。

运营措施-安全组织建设



- **看运气。**没有安全BP之前，我们找人靠在群里面问，看到回应，看不到没回应（最长**半天**）。
- **可预测。**现在每个部门、业务线建立了安全BP，我们能精确定位，事事有回应，能快速到人（平均**10min**可以回应）。

运营措施-安全组织考核

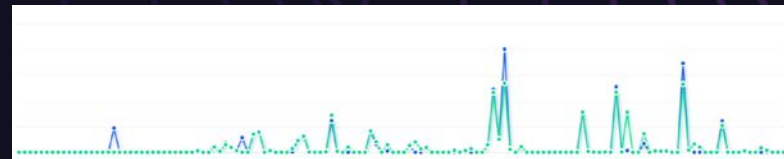
● 安全宣贯

对安全制度与安全规范进行内部宣贯

专项宣传**13**次

● 响应速度

问题发生后快速进行反馈响应



工单处理平均控制在**90**分钟内



五大
维度

● SEC工单提交量

多次提交SEC工单进行安全测试

主动安全工单占比大于
11%

● 解决速度

出现问题及时沟通发布解决方案

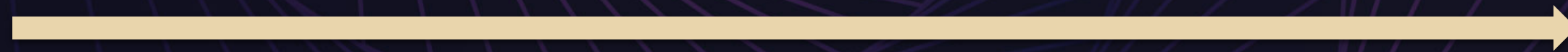
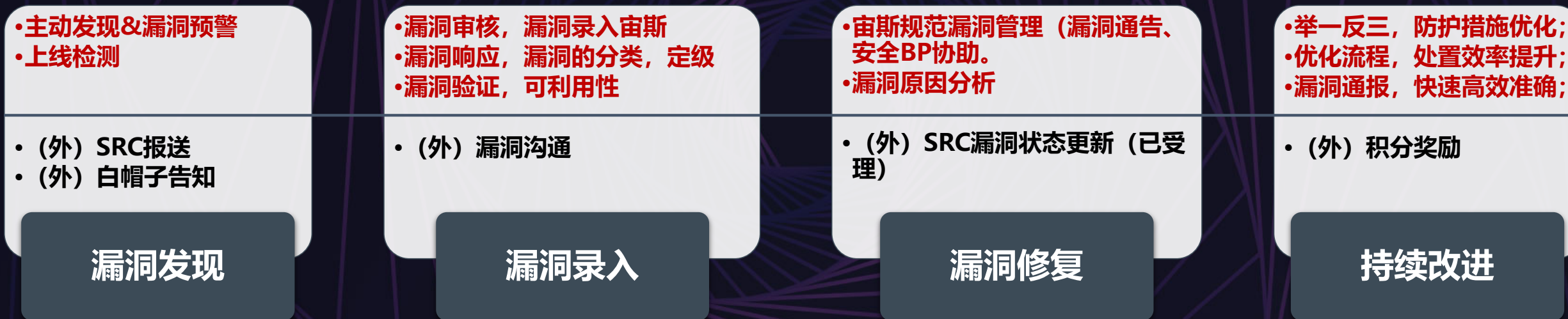
拉群沟通**50+**次

● 安全主动性

主动推动安全规范、主动提测安全评估

累计推动修复漏洞**1000+**

运营措施-安全漏洞闭环管理



安全宣传



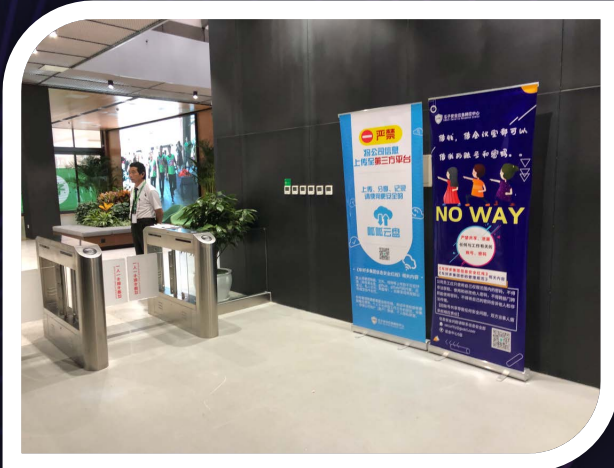
安全意识漫画 (呱呱&线下)



车好多文化社 出品



安全周宣传活动



• 安全意识的宣传渠道多样化, 覆盖不同的人
群, 宣传覆盖累计 90000+ 人次。

安全培训



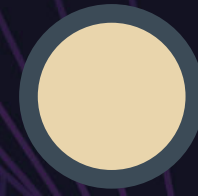
意识培训

- 新员工入职培训
- 对中后台人员安全操作培训
- 制度培训宣传培训



技术培训

- 对产品开展安全培训
- 研发组织的安全培训



专家培训

- 请外部专家进行的管理层安全培训。

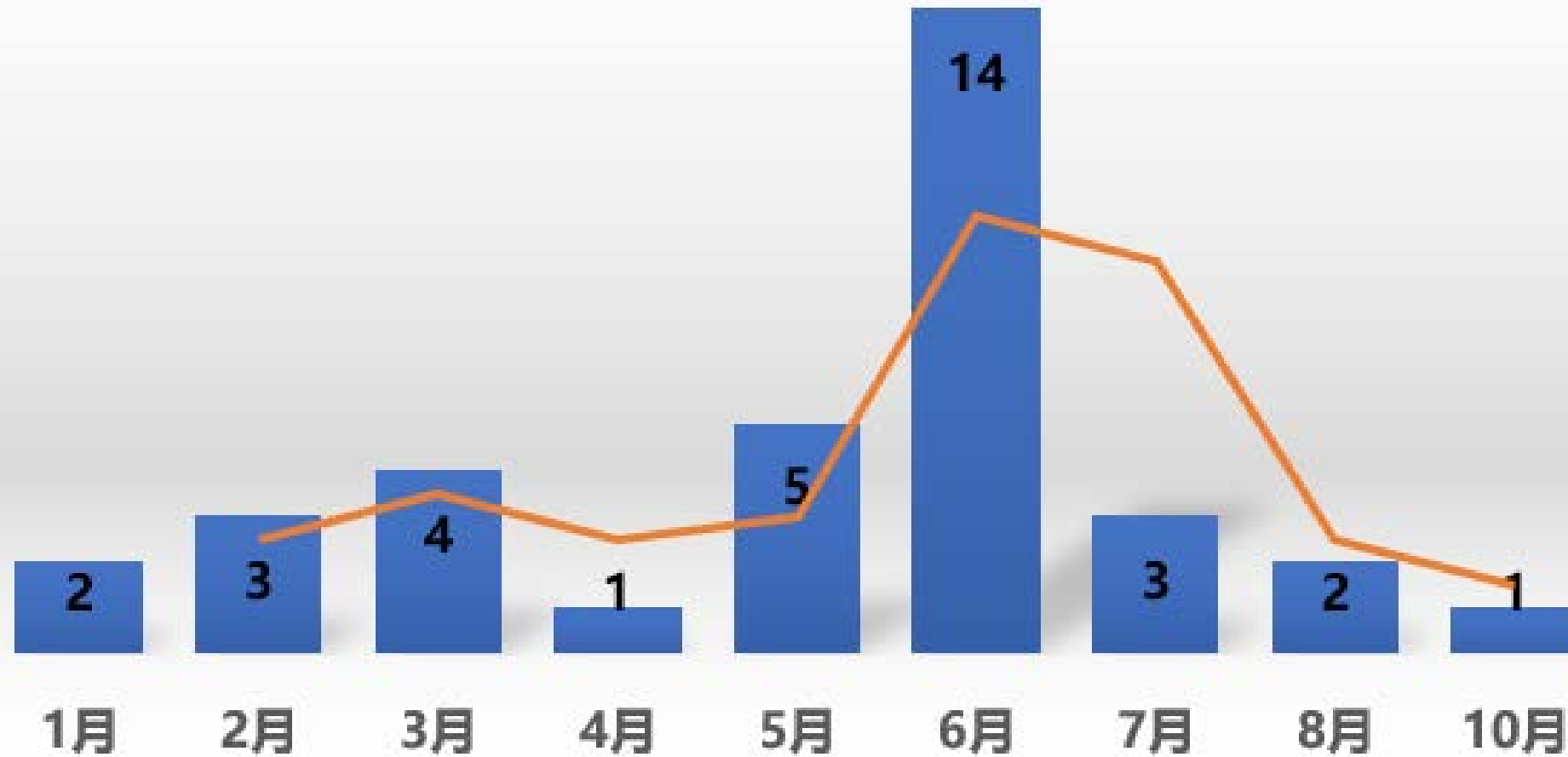
- 车好多建立瓜瓜学堂，安全运营和HR团队合作，把安全技术培训做成在线课程，要求：
 - ✓ 新入职员工全部在线学习后进行在线考试。
 - ✓ 定期组织技术培训和考试（平均每月一次）。

安全管理与事件外置

- 信息宣传
- 成立鉴
- 依据《
- 容鉴定

入职签订、日常高频次

数量趋势



安全运营的愿景

基于集中化运营平台数据驱动的自动化运营

SRC数据导入

依赖于CMDB

- 技术架构
- 管理制度
- 流程工单

安全组织

通告标准自动化

意识宣传

安全培
训覆盖
率

违规处
事件罚
率

安全考
试通过
率

可视化

数据可视化

态势可视化

溯源可视化

可感知

集中日志告警

威胁情报预警

合规达标率

可管控

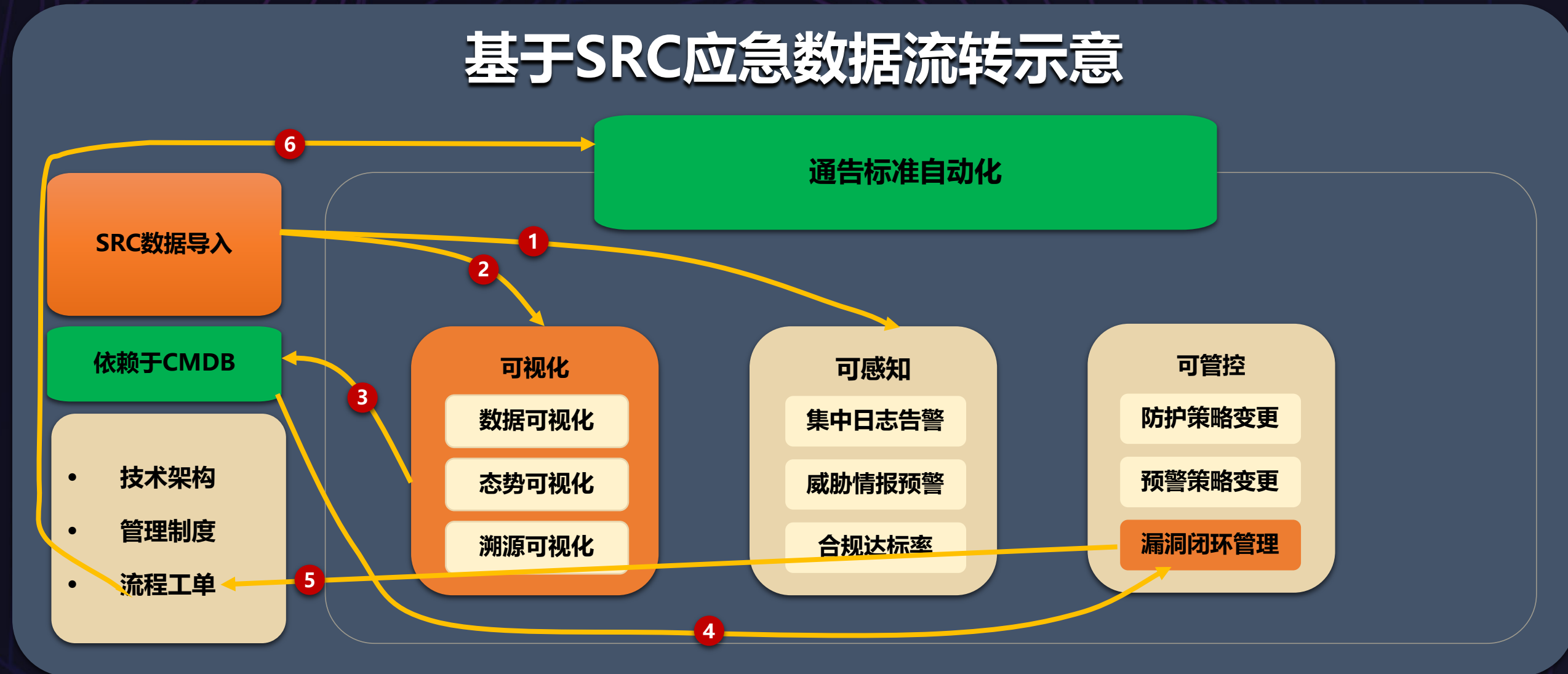
防护策略变更

预警策略变更

漏洞闭环管理

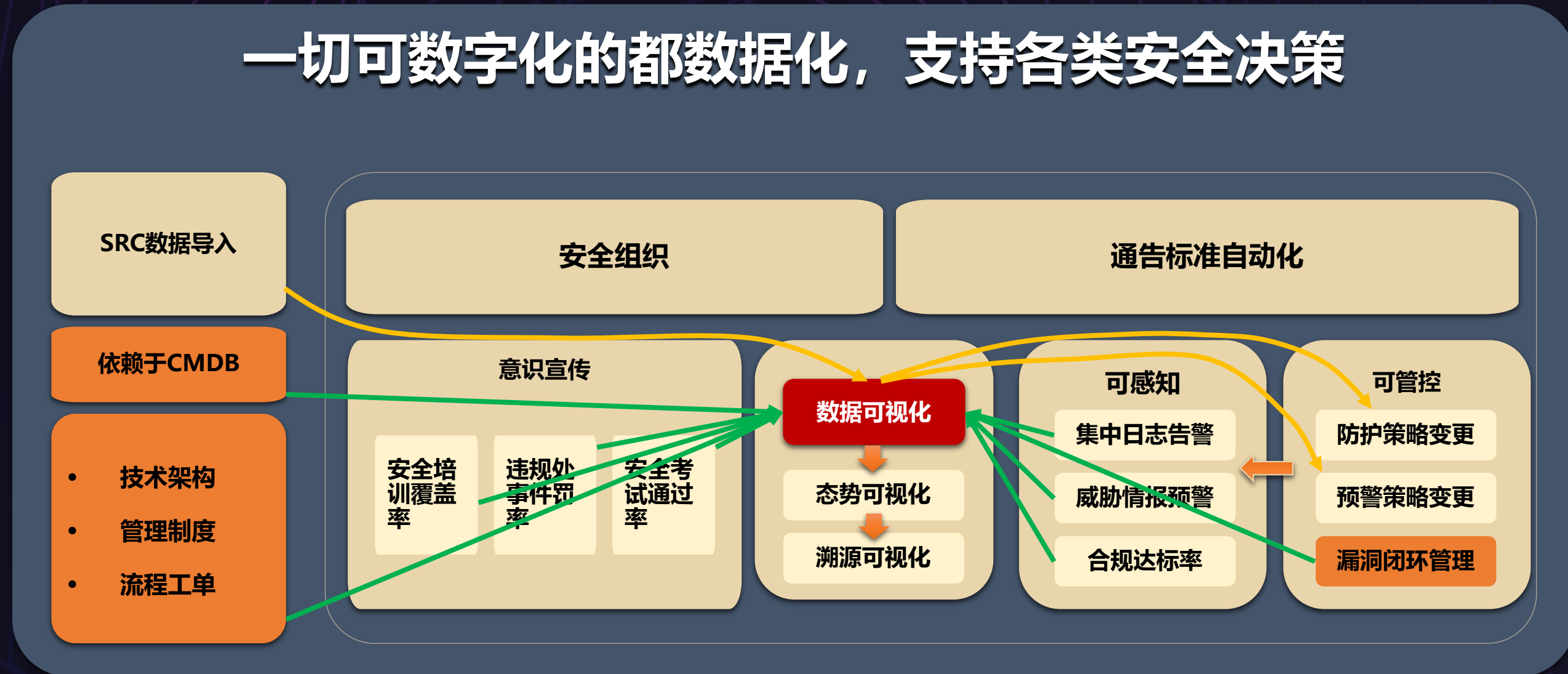
安全运营的愿景—SRC管理

基于SRC应急数据流转示意



安全运营的愿景—数字化管理

一切可数字化的都数据化，支持各类安全决策



安全运营的愿景—集中化管理

数据集中、决策集中、策略集中



后续如何做？

大家遇到白帽子捂漏洞有什么好的解决思路吗？

捍 卫 信 任 2 0 1 9 京 麒 国 际 安 全 峰 会

THANKS