车好多安全运营实践

为什么要做安全运营

通过运营发现安全的薄弱环节，驱动安全建设。

建立业务团队安全接口人，了解业务，融入业务，更好的为业务提供安全服务能力。

整合安全产品、安全工具，实现集中化、自动化和可视化的集中管控能力，遵循业务流程，输出安全价值。

京麒
国际安全峰会

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。

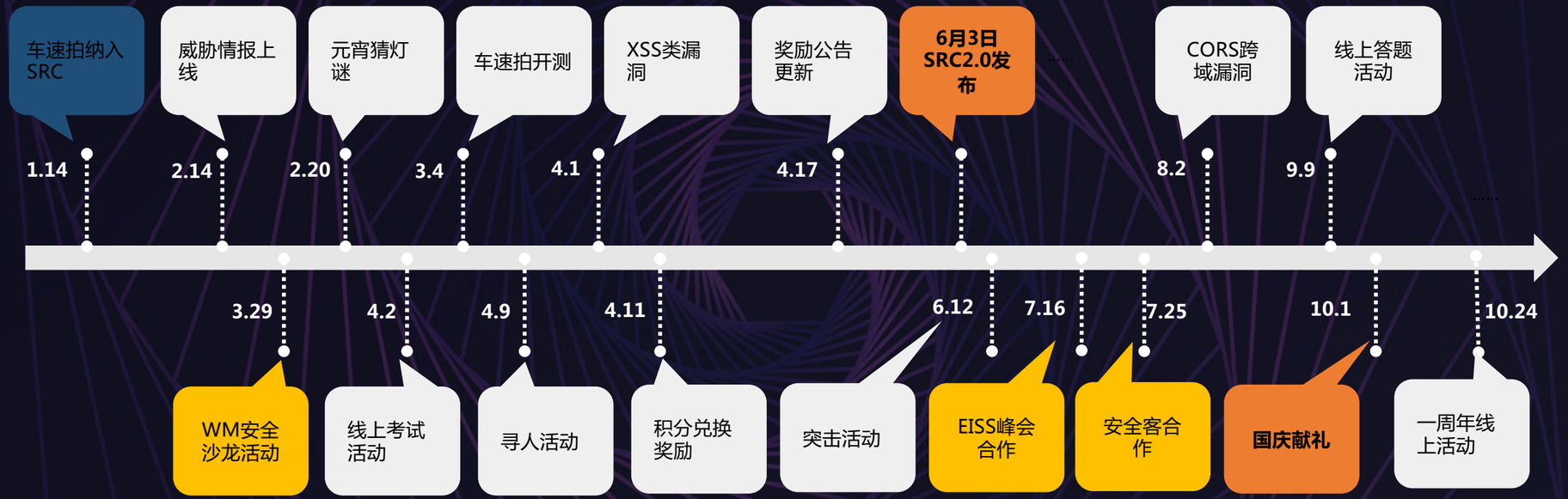
安全运营的内容

安全运营的内容

- 外部运营
  - 活动运营
  - 用户运营
  - 品牌运营

- 内部运营
  - 安全宣传
  - 安全培训
  - 违规处置

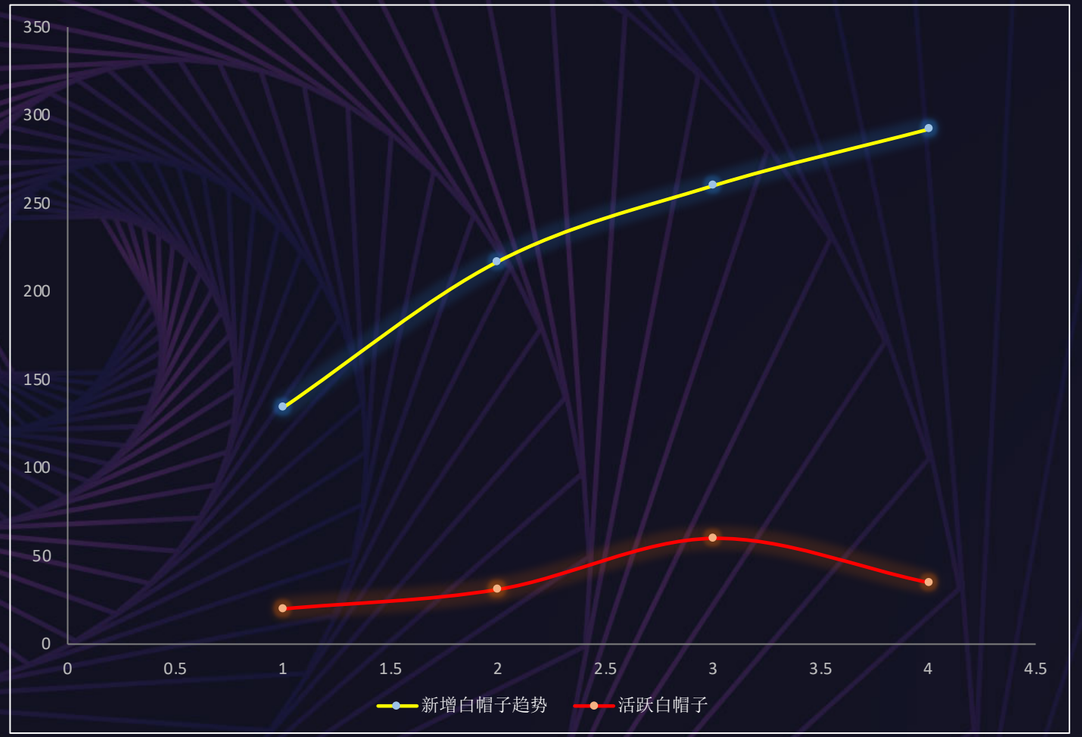
SRC活动运营



- 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

WISEMAN CONSULTING CO., LTD.

漏洞盒子

看雪

FREEBUF WWW.FREEBUF.COM

安全客 有思想的安全新媒体

补天 漏洞响应平台

安全+

嘶吼 ROARTALK

品牌影响

- 互动：25家SRC

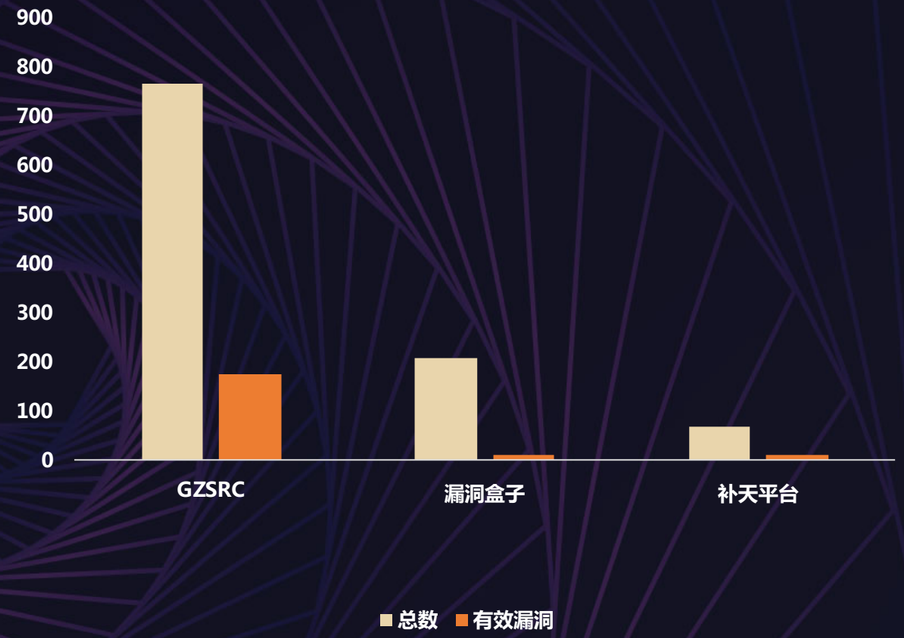
完美世界安全应急响应中心 security.wanmei.com

小米安全中心 Xiaomi Security Center

唯品会安全应急响应中心 VSRC VIP Security Response Center

CarSRC 连接·联合 保护你的每一次出行

GZSRC运营成果

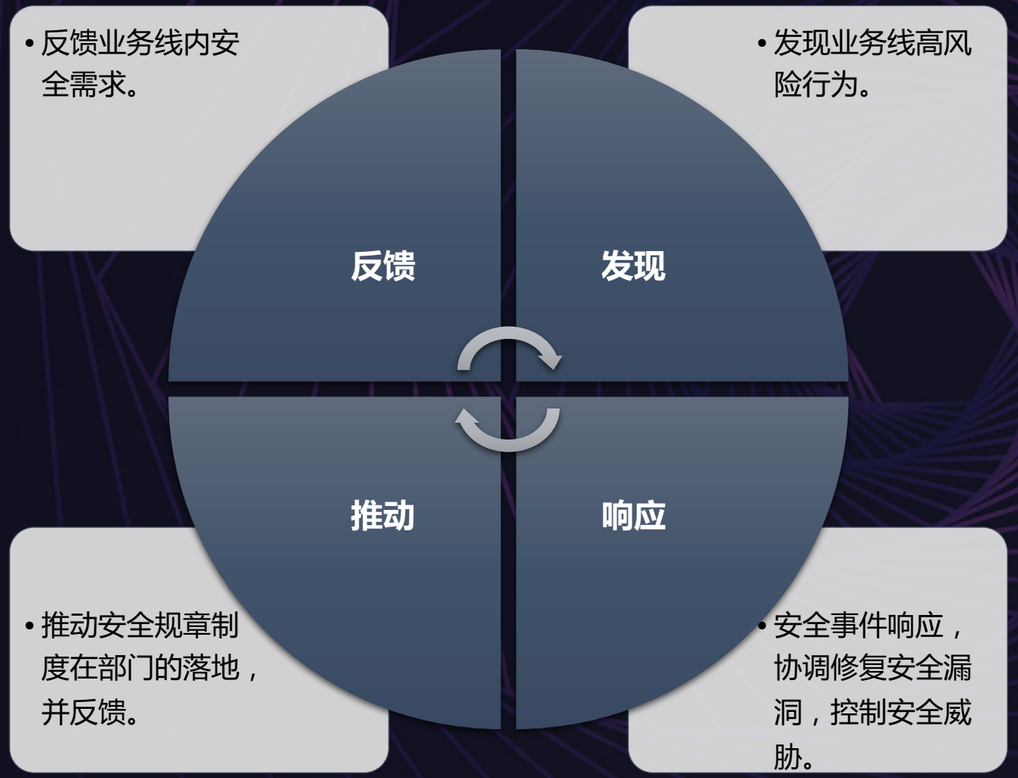


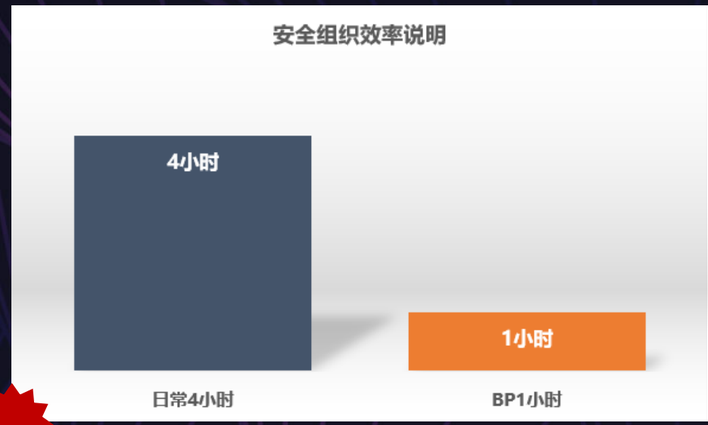
- 通过安全运营，GZSRC有效收集能力大大增强，随着安全防护手段的完善，漏洞提交量趋向减少。通过活动运营、用户运营和品牌运营，大大减少企业因为安全漏洞带来的风险。

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

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%

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

解决速度

出现问题及时沟通发布解决方案

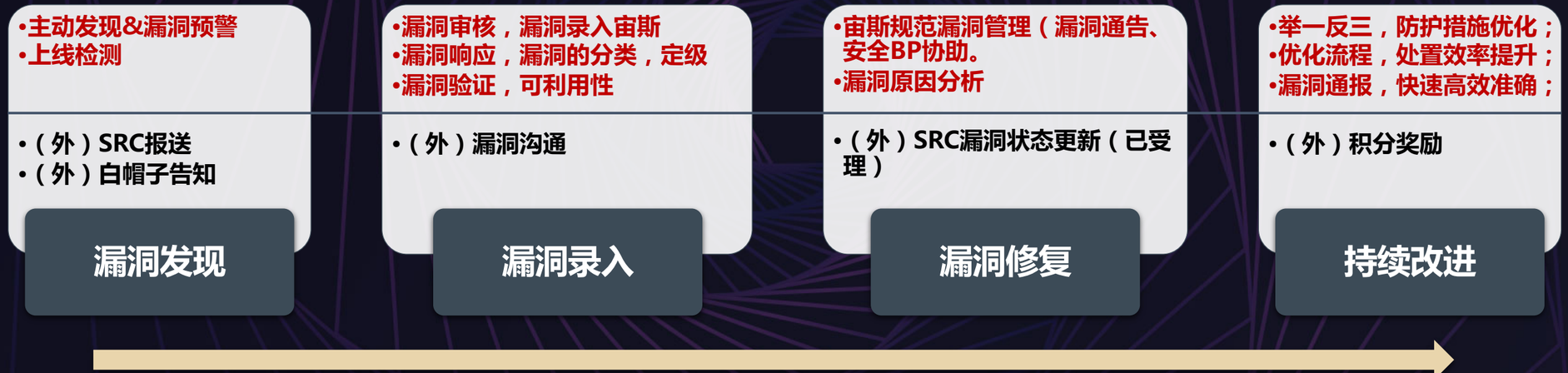
拉群沟通50+次

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）

安全周宣传活动

安全意识提升点 每周1次

- 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。

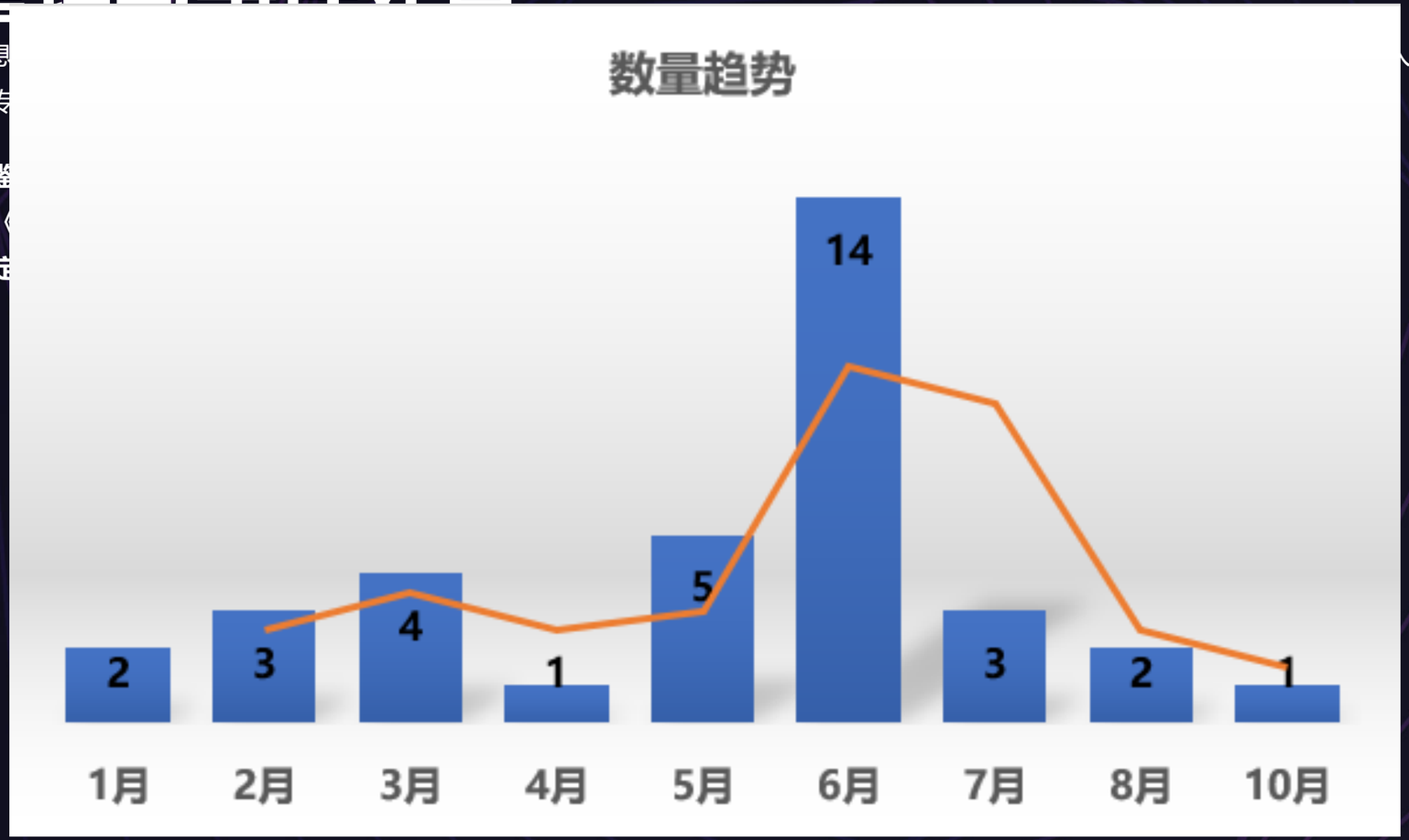
- 车好多建立瓜瓜学堂，安全运营和HR团队合作，把安全技术培训做成在线课程，要求：
  - ✓ 新入职员工全部在线学习后进行在线考试。
  - ✓ 定期组织技术培训和考试（平均每月一次）。

安全管理与事件处置

- 信息
  宣传

入职签订、日常高频次

成立鉴
依据《
容鉴定



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

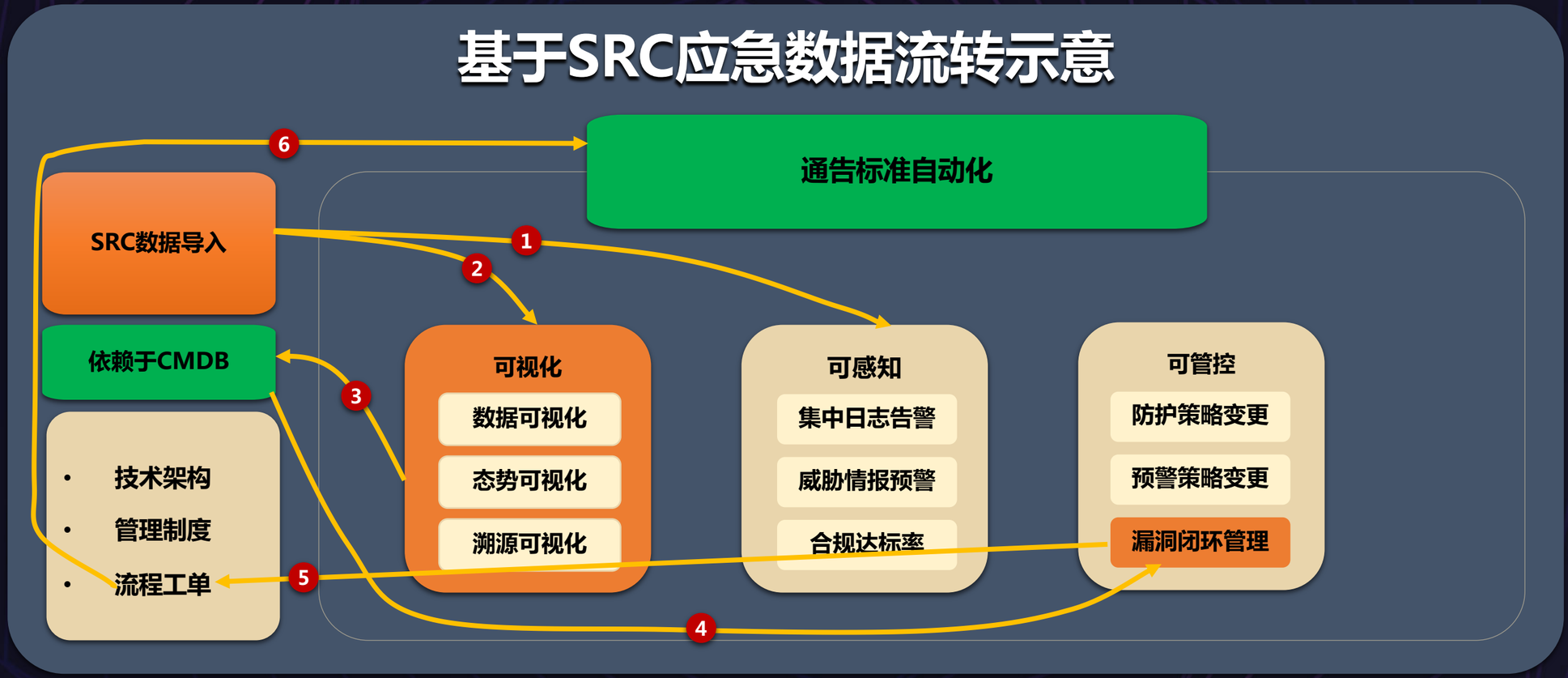
可管控

防护策略变更

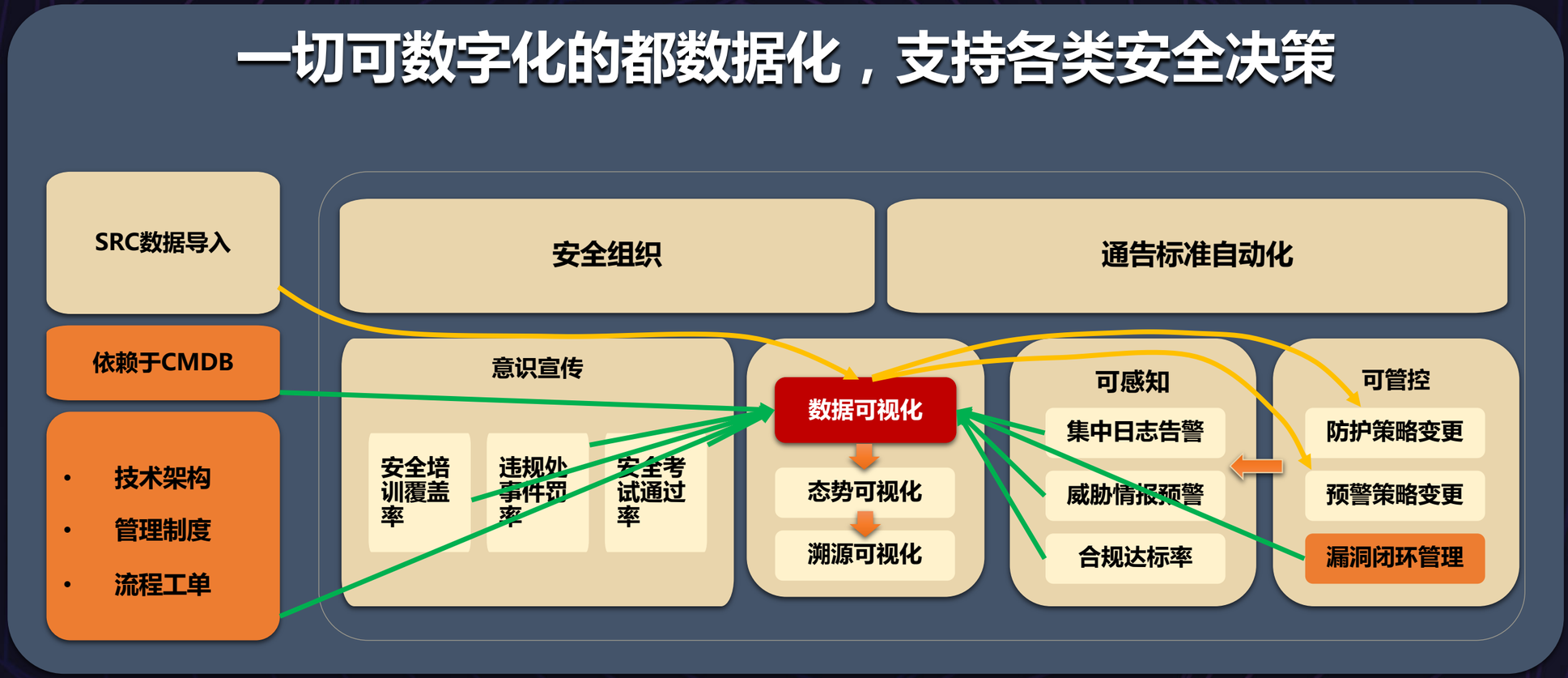
预警策略变更

漏洞闭环管理

安全运营的愿景—SRC管理



安全运营的愿景—数字化管理



安全运营的愿景—集中化管理

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？

THANKS