互联网企业安全建设落地实践

张博

同程艺龙安全负责人

关于同程艺龙

ABOUT TONGCHENG-ELONG

同程艺龙是中国在线旅行行业的创新者和领导者， 由同程旅游集团旗下同程网络与艺龙旅行网于2018年3月合并而成。以交易额计，同程艺龙位居中国在线旅行市场前三名。2018年11月26日，同程艺龙成功在香港联交所主板挂牌上市（股票代码：0780.HK）。

同程艺龙致力于打造在线旅行一站式平台，业务涵盖交通票务预订（机票、火车票、汽车票、船票等）和在线住宿预订，及多个出行场景的增值服务。截至2019年上半年，同程艺龙机票预订业务覆盖由751家国内航空公司及国际航空公司运营的超过7000条国内航线及超过120万条国际航线，住宿预订业务覆盖全球超过150万家酒店及非标准住宿，汽车票、船票业务覆盖全国约32.4万条汽车线路及超过492条航运线路。

同程艺龙拥有微信支付中的机票火车票入口和酒店入口。同程艺龙运营的小程序“同程艺龙酒店机票火车”持续位居阿拉丁月度微信小程序榜榜首。至2018年三季度末，同程艺龙平均月活跃用户数达到2.06亿。

我们的使命是“让旅行更简单、更快乐”，我们将持续运用创新科技，为用户创造简单、快捷、智能的出行服务。

成功上市后，年轻的同程艺龙开启了新的征程，将持续提升技术实力，引进优秀技术人才，以创新科技引领在线出行服务创新，率先实现从OTA到ITA（Intelligent Travel Assistant）的升级。

同程艺龙

7000+ 条

国内机票业务覆盖超过7000条国内航线

120W+ 条

国际机票业务覆盖超过120万条国际航线

32W+ 条

国内汽车票业务覆盖全国32万条汽车线路

492+ 条

船票业务覆盖全国300条航运线路

150W+ 家

住宿业务覆盖全球超过150万家酒店及非标准住宿

2.06 亿

2018年三季度末平均月活跃用户数达到2.06亿

CONTENTS

互联网企业安全主体责任

责权一致：主体责任彰显企业担当

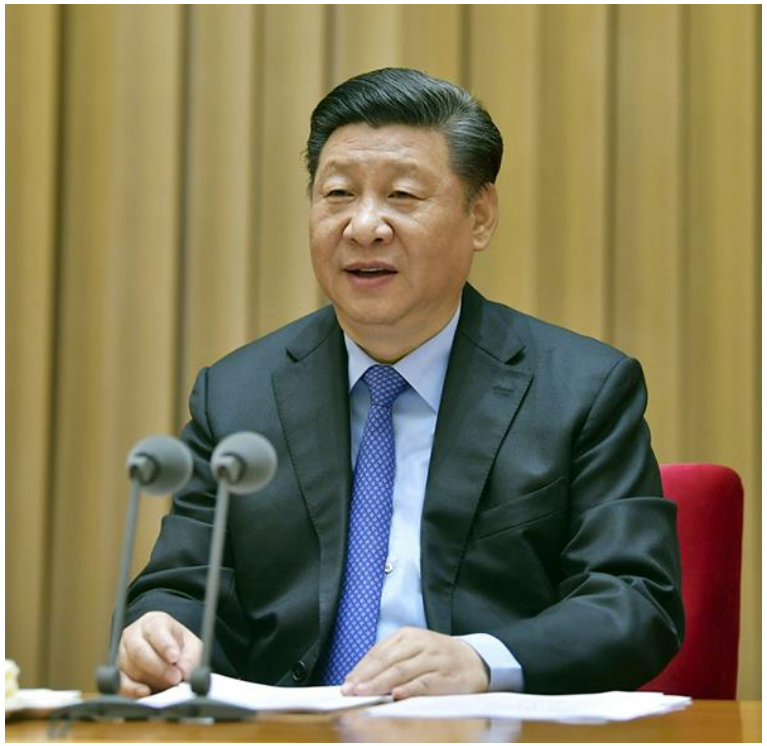
2018年4月20日至21日，习近平总书记在全国网络安全和信息化工作会议上提出：

要坚定不移支持网信企业做大做强，加强规范引导，促进其健康有序发展。企业发展要坚持经济效益和社会效益相统一，更好承担起社会责任和道德责任。

要落实关键信息基础设施防护责任，行业、企业作为关键信息基础设施运营者承担主体防护责任，主管部门履行好监管责任。

要压实互联网企业的主体责任，决不能让互联网成为传播有害信息、造谣生事的平台。要加强互联网行业自律，调动网民积极性，动员各方面力量参与治理。

要依法严厉打击网络黑客、电信网络诈骗、侵犯公民个人隐私等违法犯罪行为，切断网络犯罪利益链条，持续形成高压态势，维护人民群众合法权益。



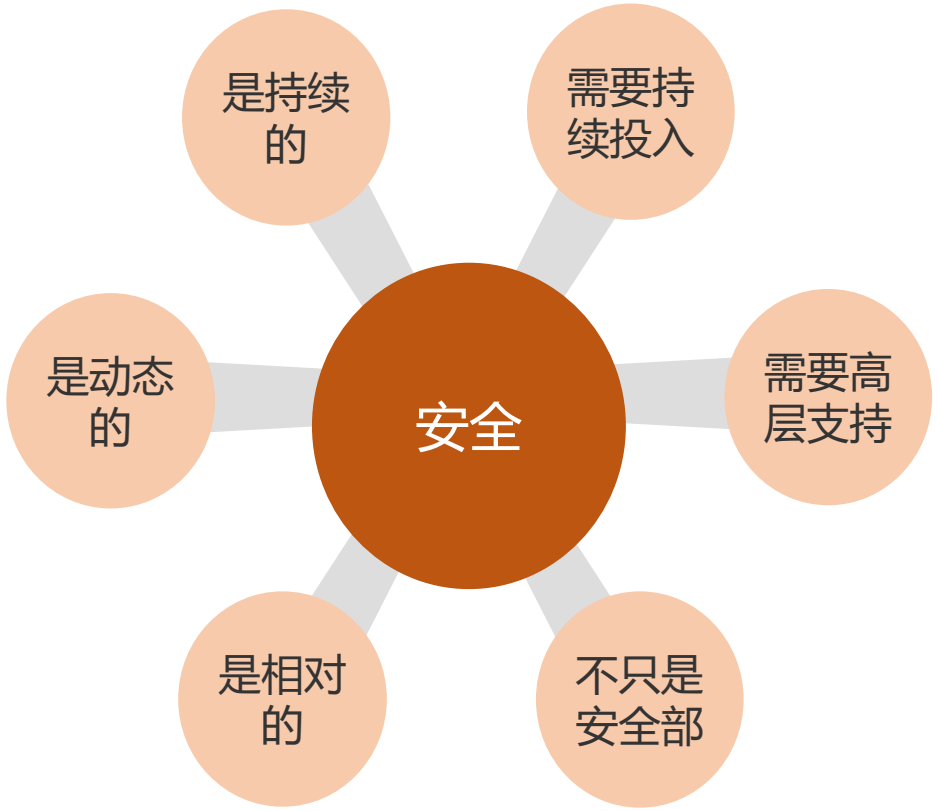
服务、便利　　安全、可靠　　社会责任

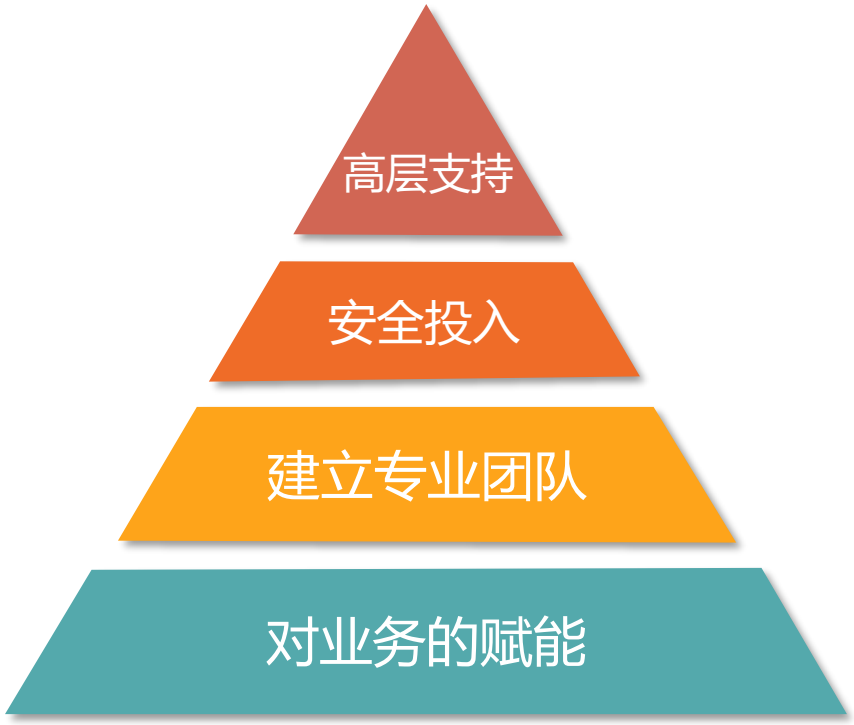
互联网企业安全工作的特点

安全很重要，但是……

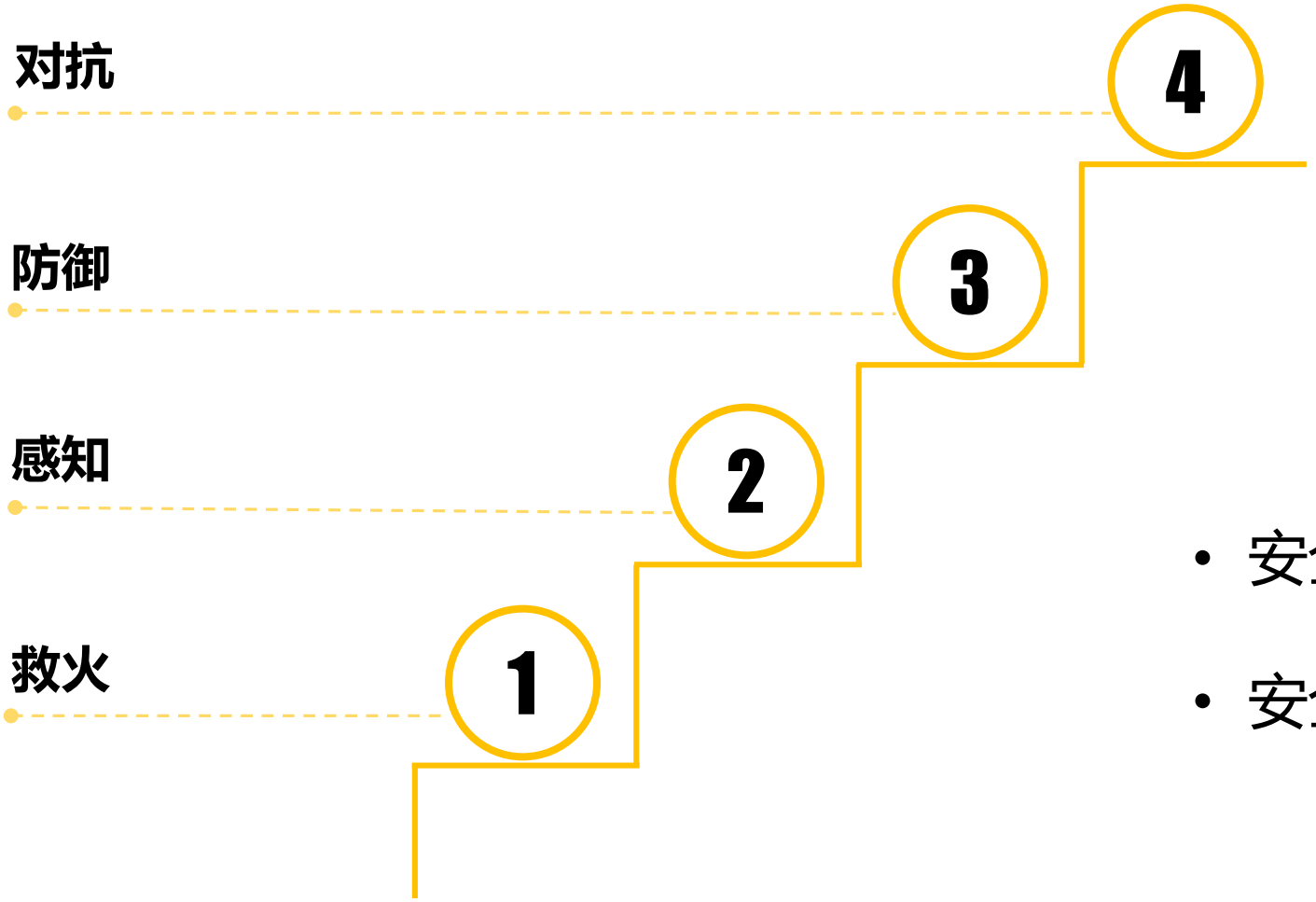
- 流量大，变化快，开发上线迭代快 → 传统安全手段失效，变化带来更大风险
- 业务优先，BG/BU制，话语权 → 安全解决方案复杂，难以推动和落地
- 安全实用主义，最小成本最大收益 → 安全、可用性、易用性/便利、成本/收益
- 自建团队，研发能力和影响力 → 人员招聘、影响力、成长空间、稳定性

互联网企业安全架构——树立正确的安全观





互联网企业安全架构——安全能力演进



- 安全体系分布推进
- 安全能力逐步提升

互联网企业安全架构——安全建设

安全团队：团队规模；角色构成；内部安全组织

安全组织

识别和处置能力；感知和响应能力；安全自动化平台化
安全建设和运营能力；研究和学习能力

安全能力

安全规划；安全体系完整性；安全管理和技术体系结合

安全体系

持续运营；精细化运营；运营可量化可视化；安全运营落地

安全运营

明确信息安全方面的职责和义务
安全意识教育和文化建设

安全意识

互联网企业安全架构——团队方向

互联网企业安全架构——总体设计

安全体系

安全管理体系
- 制度、策略、流程
- 资产管理
- 持续改进

安全意识培训
- 管理层
- 重要岗位、IT

合规建设
- 国家法律、标准
- 等保测评
- 行业安全认证
- 监管和重大保障
- 国际标准和认证

业务安全

会员安全系统
- 会员加固
- 机器识别
- 持续认证
- 指纹库
- 持续验证

数据安全

线下数据风险
- 终端&网络DLP
- 可信计算
- EMM
- 大数据在线分析
- 权限控制

数据地图
- 数据识别
- 分级分类
- 敏感标记
- 工单
- 数据流关联
- 数据血缘
- 所有者
- 数据目录

线上数据风险
- 密钥管理
- 权限管理
- 应用接口数据监控
- 数据库审计
- 隐私数据加密
- 隐私数据脱敏

第三方数据风险
- 数据接口监控
- 水印染色
- 可信计算
- 安全审计

基础安全

漏洞检测
- 漏洞检测平台
- 代码审计平台

防御能力
- 应用防火墙
- 安全加固

感知能力
- 态势感知
- 主机入侵检测

控制能力
- AAAA
- 身份认证

安全运营

安全影响力
- 安全门户
- SRC平台
- 安全宣传&培训

预警&检测
- 安全平台预警
- SDL
- 风险整改跟进

应急响应
- 安全演练
- 安全事件应急
- 安全事件复盘

CONTENTS

国家要求

合规要求

监管趋严

业务方的共鸣和重视

01 事件驱动：正确“利用”安全问题

02 内部运营：应急、监控感知、风险治理

03 安全组织：安全**共赢**，内部生态建立

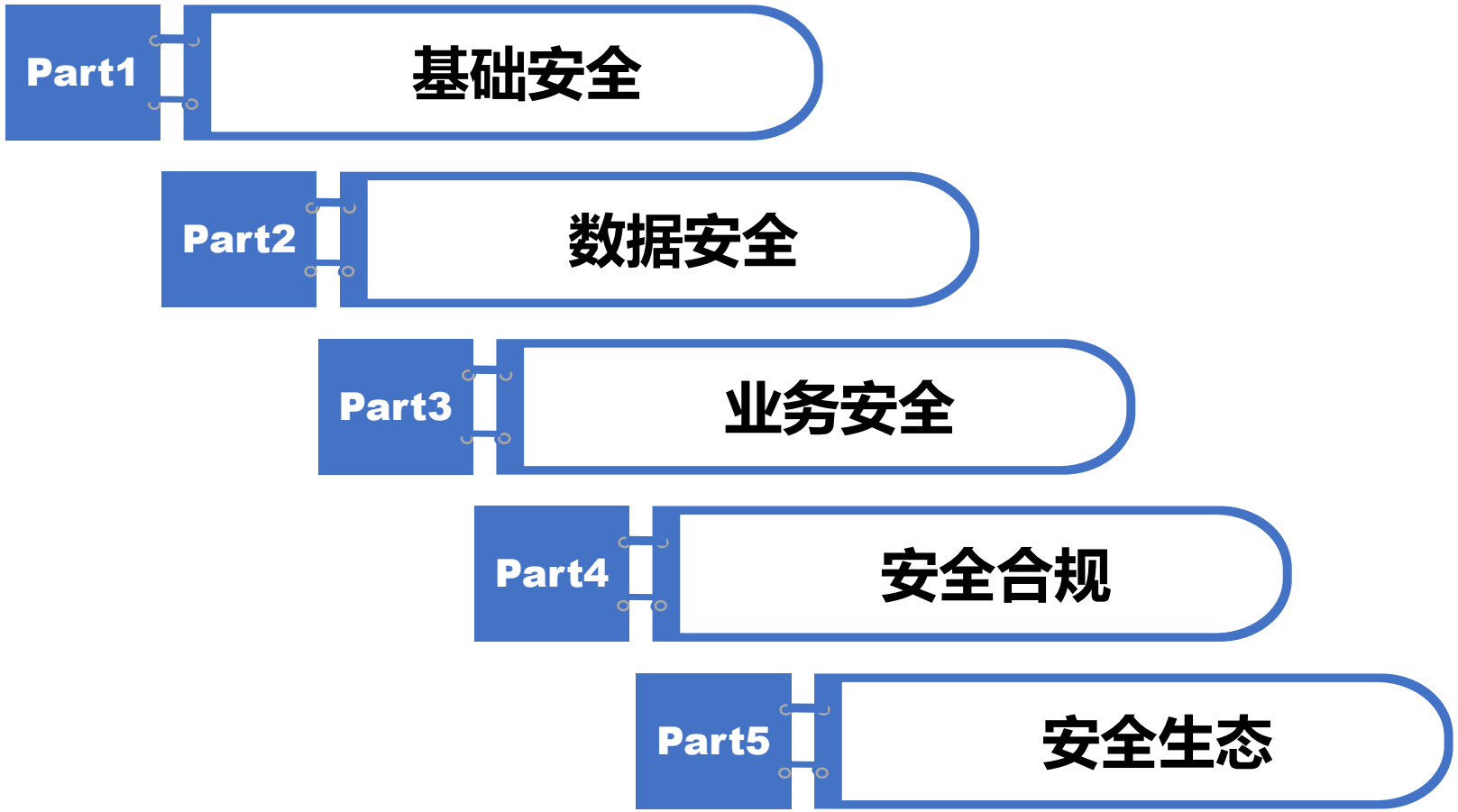
04 安全文化：安全奖惩，影响力建设

人和

- 内部团队建设：快速搭建团队，团队文化，责任心，靠谱
- 外部行业关系：朋友圈很重要，白帽子、同行、第三方、社区、……
- 监管层对接：公安、网信、工信、行业监管机构
- 行业生态建立：上下游（供应商、分销商、保险公司、代理机构）

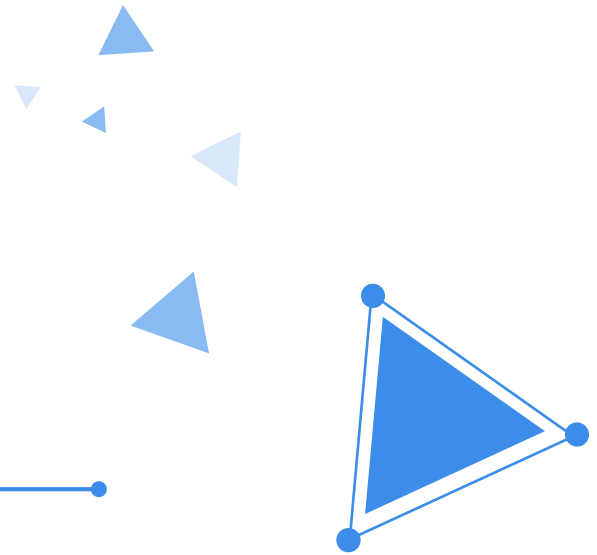
CONTENTS

安全建设落地经验分享

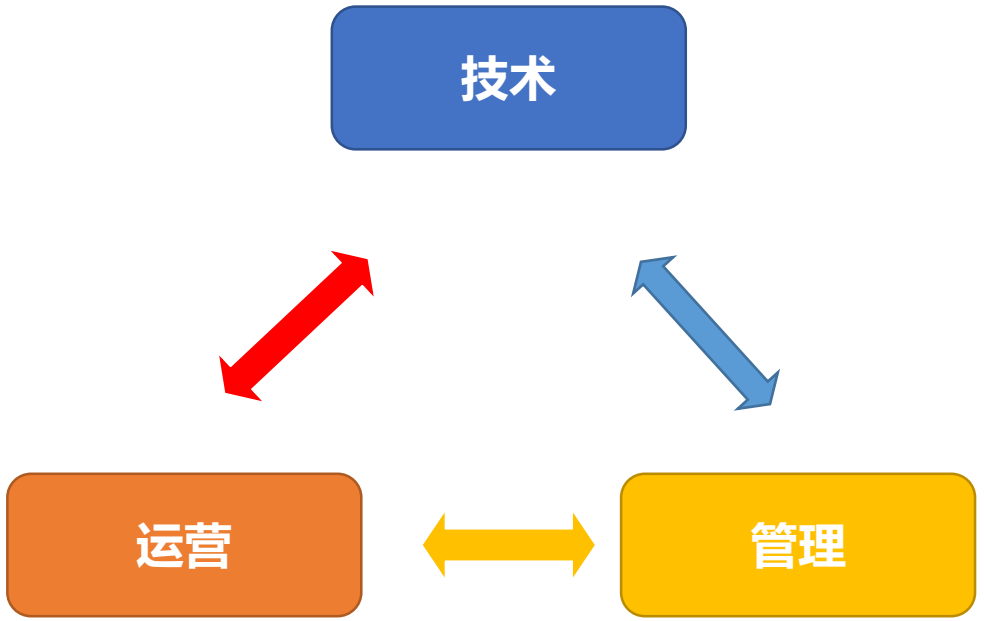


01 Part One

基础安全能力



A、风险治理能力



技术

风险发现能力，风险管理平台，安全工单

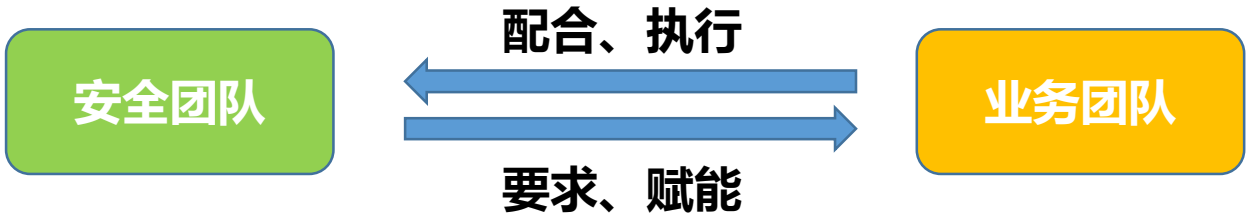
运营

风险管理制度，安全接口人

管理

定量运营指标，可视化，风险跟进机制

SDL/DEVSECOPS/三同步

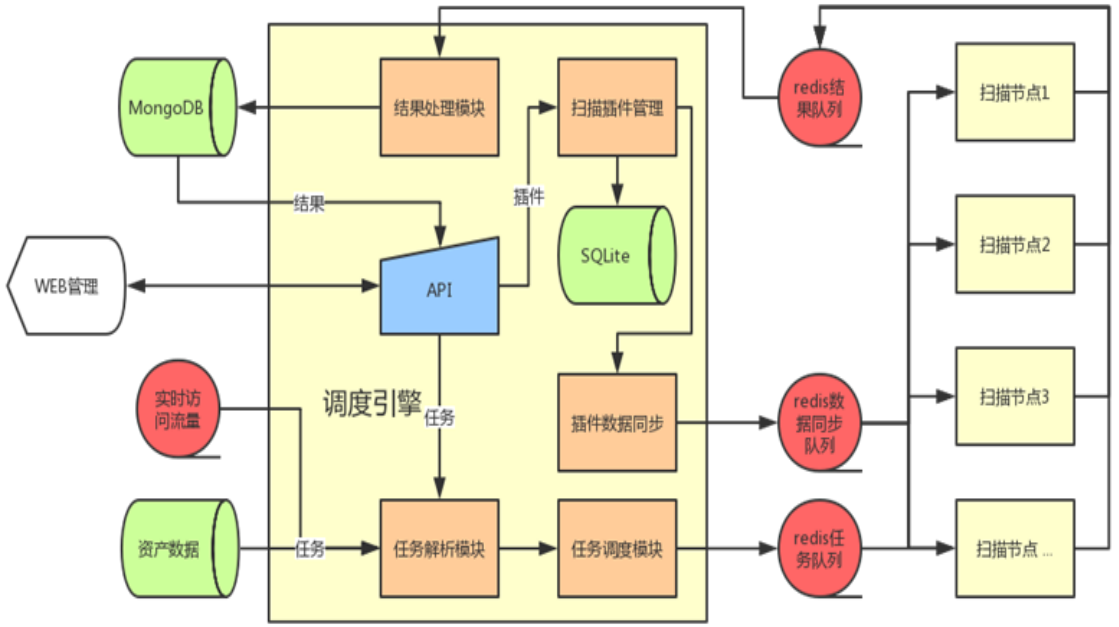


Training	Requirements	Design	Implementation	Verification	Release	response
安全意识培训	代码安全规范	安全需求分析	黑盒检测服务	QA检测流程	白盒代码审计	黑盒漏洞检测
代码规范培训	安全测试规范	安全功能	白盒检测服务	黑盒检测插件	上线卡点	资产
日常宣传	漏洞管理规范	组件版本	人工检测服务			流量
关键岗位考核		安全策略				爬虫
						风险跟进
						风险工单

关键词：流程、工具、培训

分布式安全扫描平台

- **业务资产识别（自适应资产变化）**
  CMDB+端口扫描+流量+爬虫
- **分布式扫描（自适应任务调度）**
  调度引擎+单业务控制+限速机制
- **漏洞检测规则（自适应漏洞规则）**
  通用组件+通用漏洞+逻辑问题+0day
- **安全风险发现**
  敏感后台对外，风险服务，接口，弱口令等……

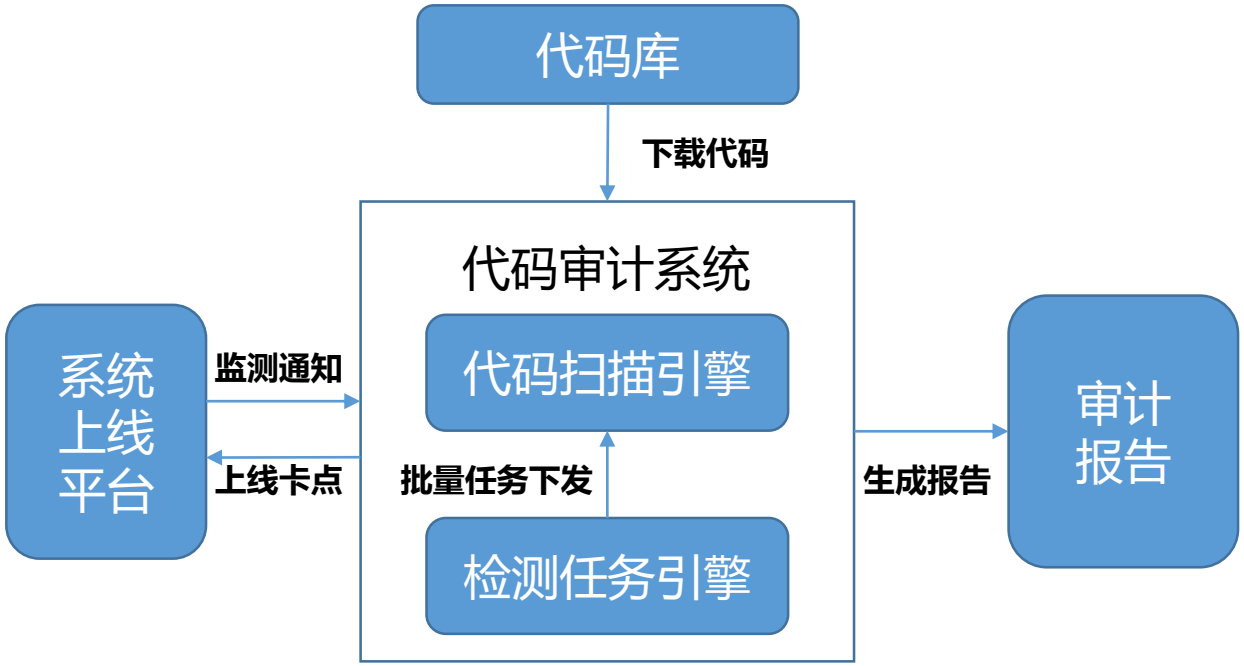


赋能业务研发和QA使用安全检测工具，安全风险发现前移

代码审计平台

- **上线平台对接**
  - 系统上线触发扫描任务
  - 根据扫描结果执行上线动作
- **批量自动化扫描**
  - 任务调度，批量扫描效率最大化
  - 代码库自动下载代码
- **漏洞检测规则**
  - 通用组件+通用漏洞+逻辑问题+0day
  - 定制扫描规则

系统上线和迭代，自动检测，卡点



B、监控感知能力

A 内部

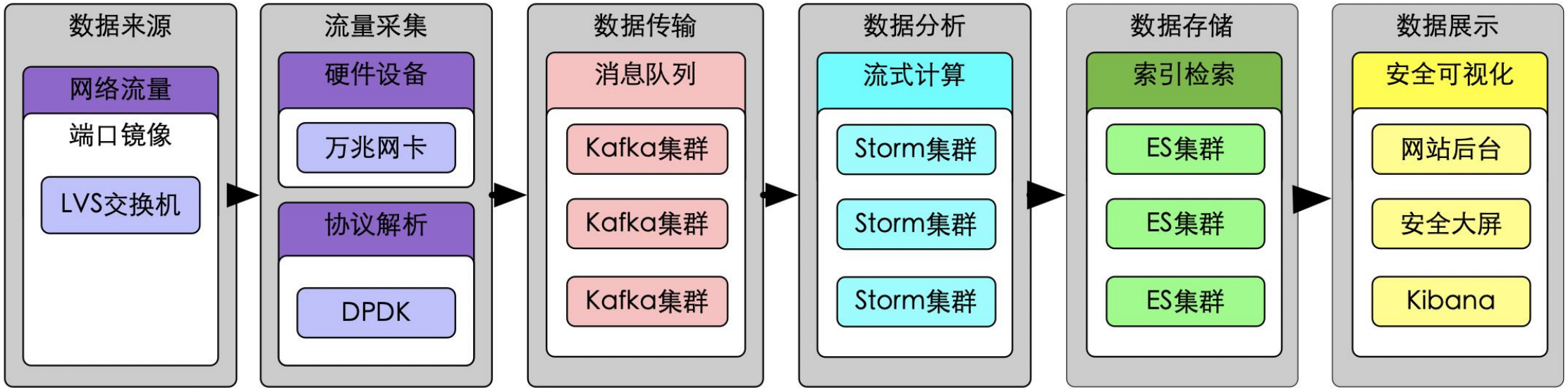
态势感知
NIDS
HIDS

B 外部

暗网监控
网盘监控
GitHub监控
威胁情报

流量 + 爬虫 + 情报 + 日志 + Agent

网络侧入侵检测平台


数据来源
网络流量
端口镜像
LVS交换机
流量采集
硬件设备
万兆网卡
协议解析
DPDK
数据传输
消息队列
Kafka集群
Kafka集群
Kafka集群
数据分析
流式计算
Storm集群
Storm集群
Storm集群
数据存储
索引检索
ES集群
ES集群
ES集群
数据展示
安全可视化
网站后台
安全大屏
Kibana

主机入侵检测平台

资产识别 IP、MAC、操作系统，系统账号，软件，进程，web框架 A

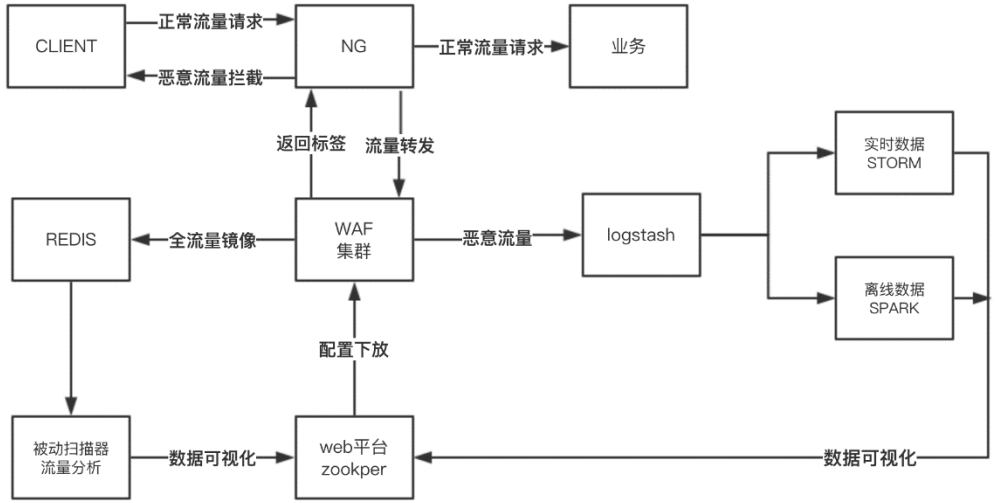
B WebShell、系统后门、本地提权、爆破、内网探测、系统漏洞、弱口令、文件篡改 **风险发现**

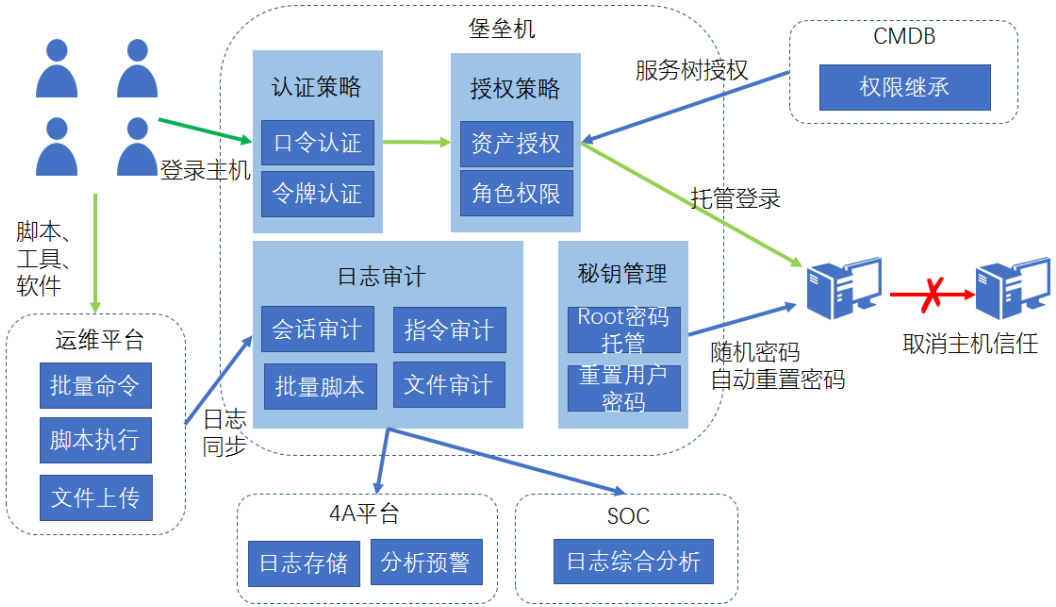
应急响应 应急工具、批量执行脚本、同类系统定位 C

C、综合防控体系

WAF

边界实时拦截
通用漏洞应急
攻击监控

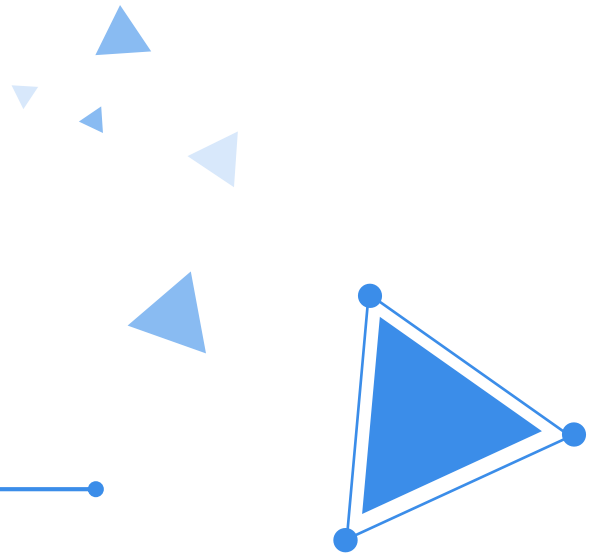




内网权限

身份认证鉴权
操作命令审计
密码保护

02 Part Two
数据安全能力

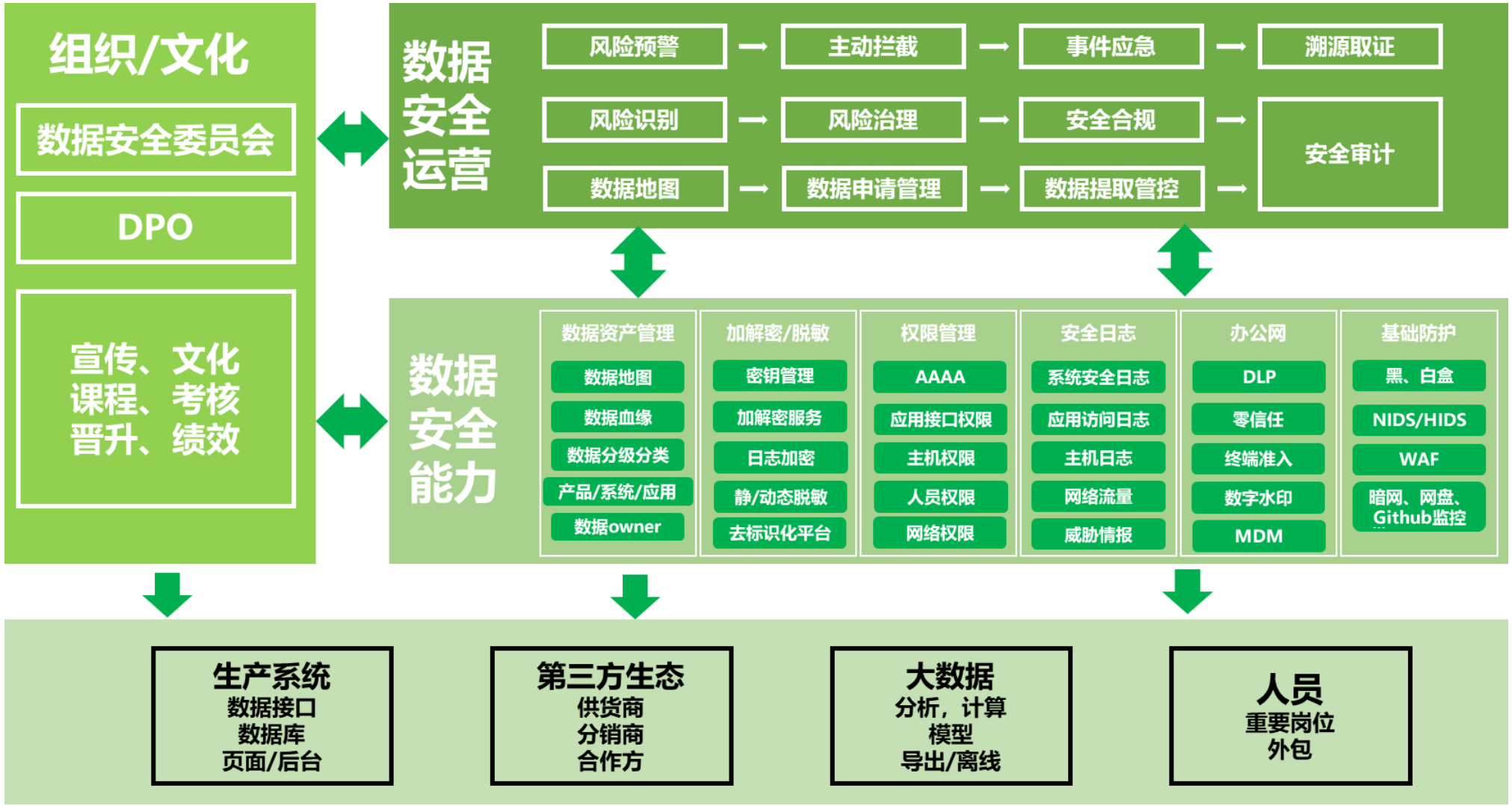


数据安全体系建设：全生命周期防护，结合业务场景落地

数据采集	数据存储	数据使用	数据传输/分享/归档	数据销毁
APP安全 数据分级分类 数据安全风控	数据保护 数据安全域 防爬技术 日志存储	数据访问权限控制 终端安全管控 移动安全 后台数据脱敏	数据/文件交换 IM/邮件安全防护 网络层保护 第三方数据防护 数据水印	硬盘销毁 文件粉碎

安全预警/审计/溯源

数据安全架构


组织/文化
数据安全委员会
DPO
宣传、文化
课程、考核
晋升、绩效
数据安全运营
风险预警
主动拦截
事件应急
溯源取证
风险识别
风险治理
安全合规
安全审计
数据地图
数据申请管理
数据提取管控
数据安全能力
数据资产管理
数据地图
数据血缘
数据分级分类
产品/系统/应用
数据owner
加解密/脱敏
密钥管理
加解密服务
日志加密
静/动态脱敏
去标识化平台
权限管理
AAAA
应用接口权限
主机权限
人员权限
网络权限
安全日志
系统安全日志
应用访问日志
主机日志
网络流量
威胁情报
办公网
DLP
零信任
终端准入
数字水印
MDM
基础防护
黑、白盒
NIDS/HIDS
WAF
暗网、网盘、Github监控
生产系统
数据接口
数据库
页面/后台
第三方生态
供货商
分销商
合作方
大数据
分析，计算
模型
导出/离线
人员
重要岗位
外包

用户数据安全：日志审计

- **风险告警**

  对重要系统后台实现异常行为风险告警

  人工规则+机器学习

- **取证溯源**

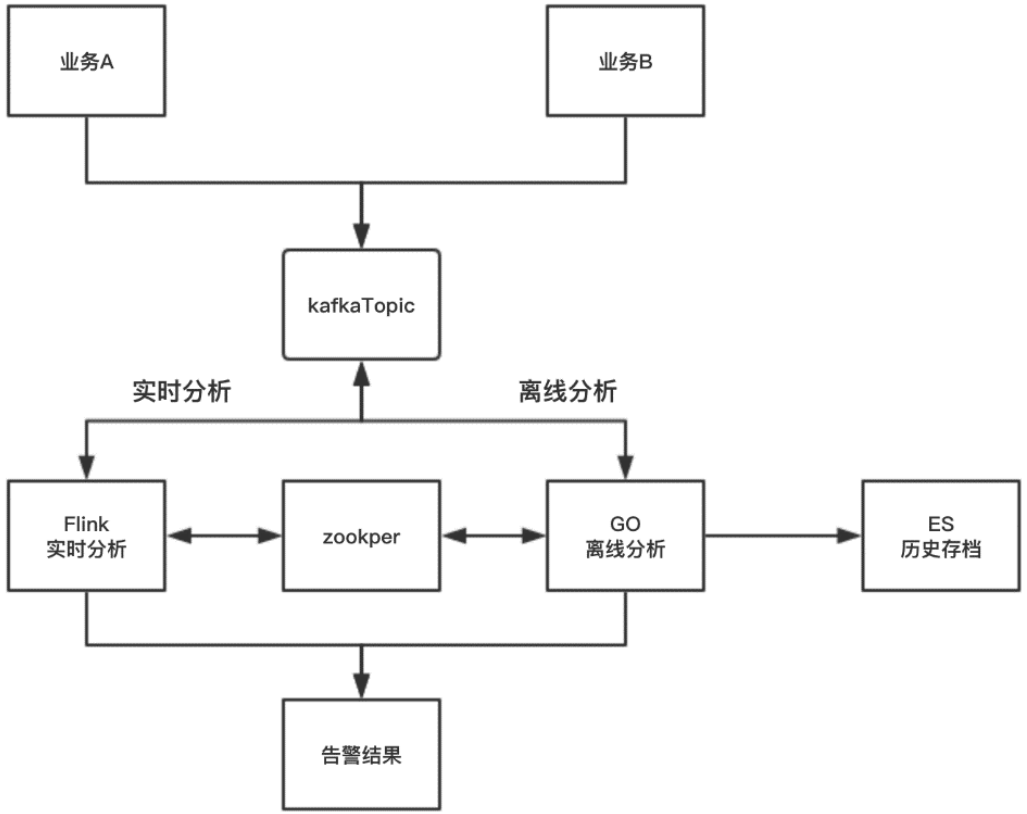
  多种事件关联，还原整个事件

  保存原始日志和证据

- **应用数据网关**

  应用接口调用审计

  数据访问使用审计

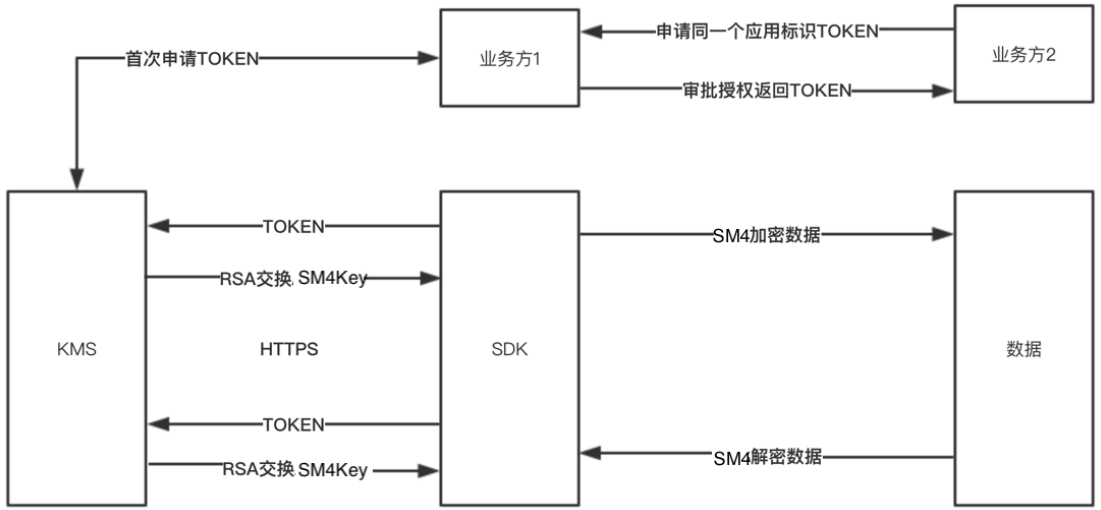


用户数据安全：加解密/密钥管理

加解密和密钥管理：

+ 加解密服务
+ 密钥申请，存储，分发
+ 日志敏感信息加密

自研加解密服务（SDK），业务集成。
密钥统一申请和分发，跨业务解密通过平台统一授权，与工单系统结合。
日志平台集成加解密服务，日常查询敏感字段被加密，查询需申请。



用户数据安全：脱敏/去标识化

数据脱敏

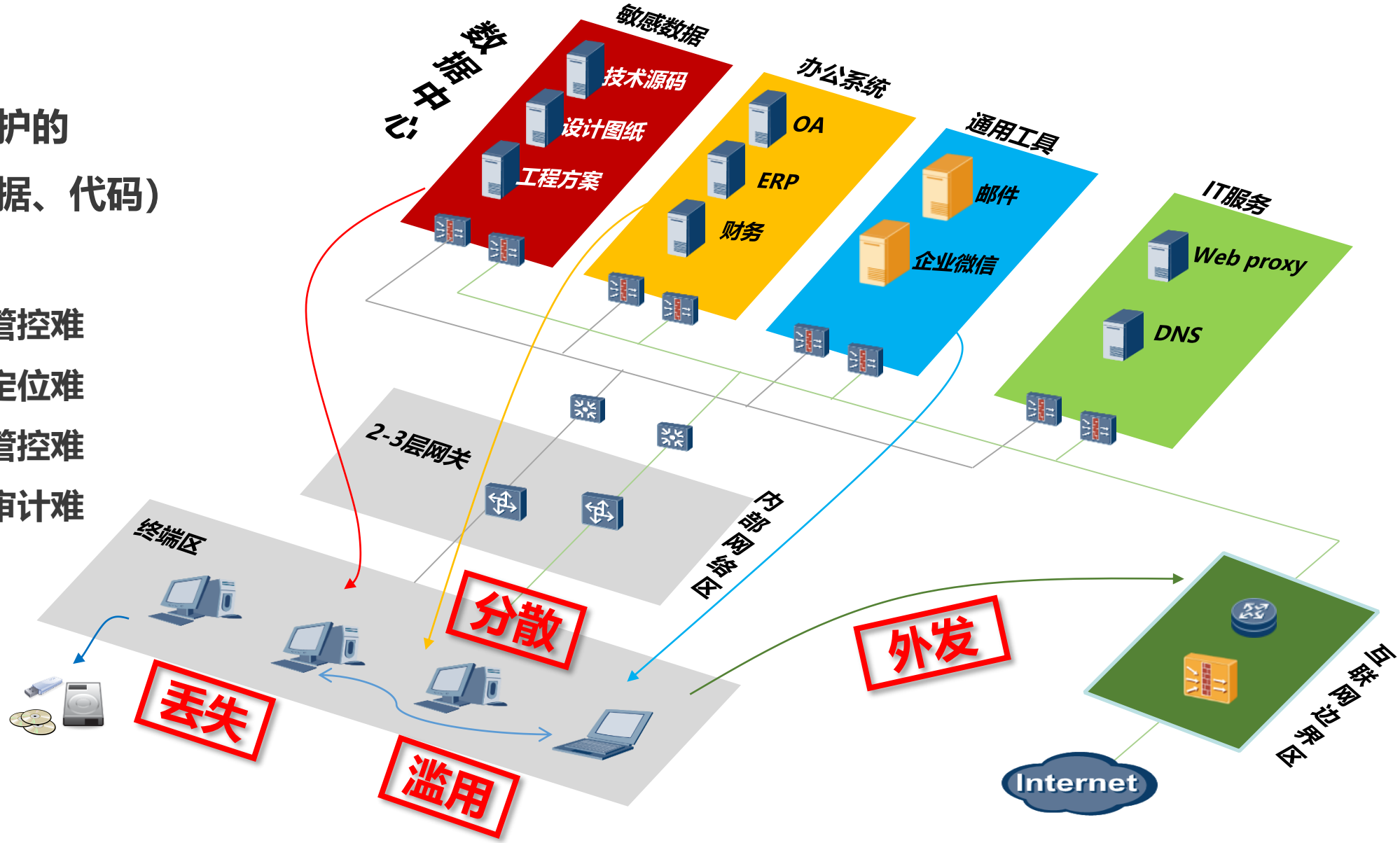
办公网数据安全保护

核心数据保护的

（文件、数据、代码）

难题：

- **办公设备管控难**
- **关键数据定位难**
- **数据泄密管控难**
- **数据预警审计难**



用户数据安全：数据防泄漏

DLP

cirrus gate 思睿嘉得

网络　终端　邮件

数据梳理 → 使用场景 → 保护动作 → 事件处置

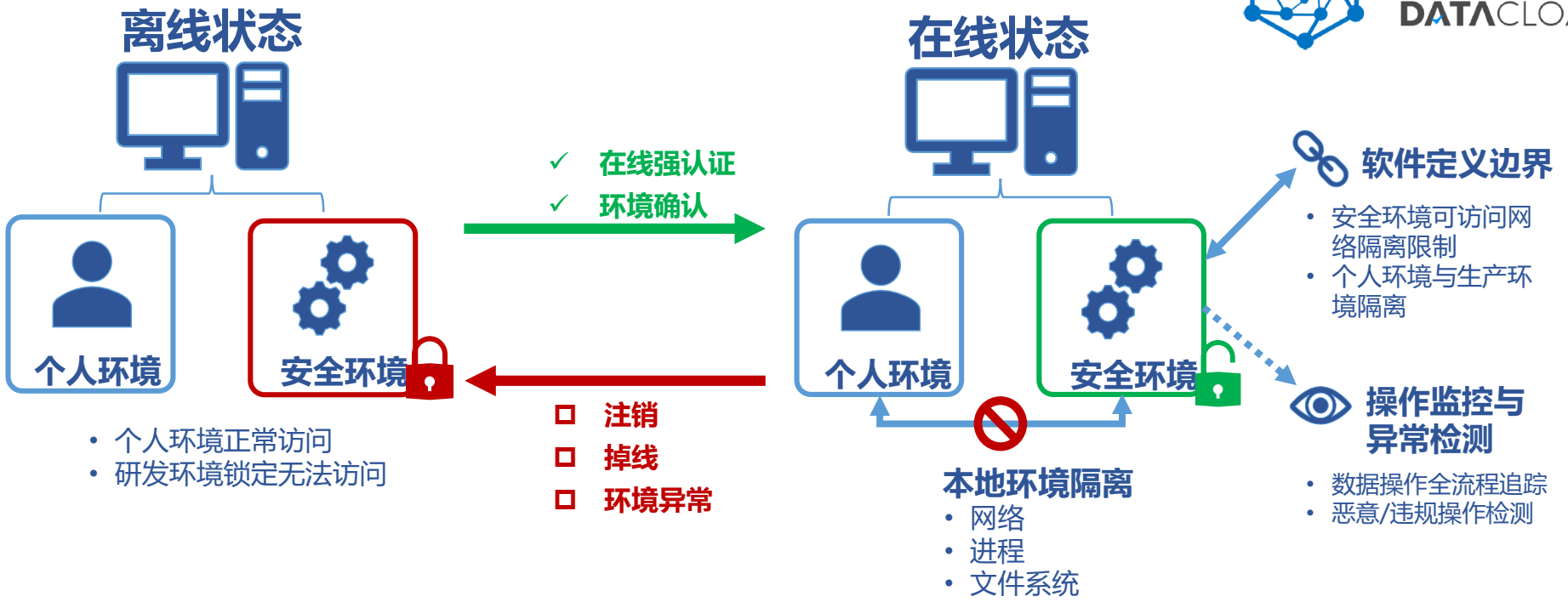
数据	用户	途径	许可	操作行为	响应动作	处置
 分类分级	用户 部门 设备	协议 程序 外设	放行 阻断	打开 复制 剪切 移动 外发 截屏	强制拒绝 主动放弃 质问放行 规则放行 告警记录	事件状态 事件判断 人工处置 规则处置 合规 风控 法务 人事

+

EMM

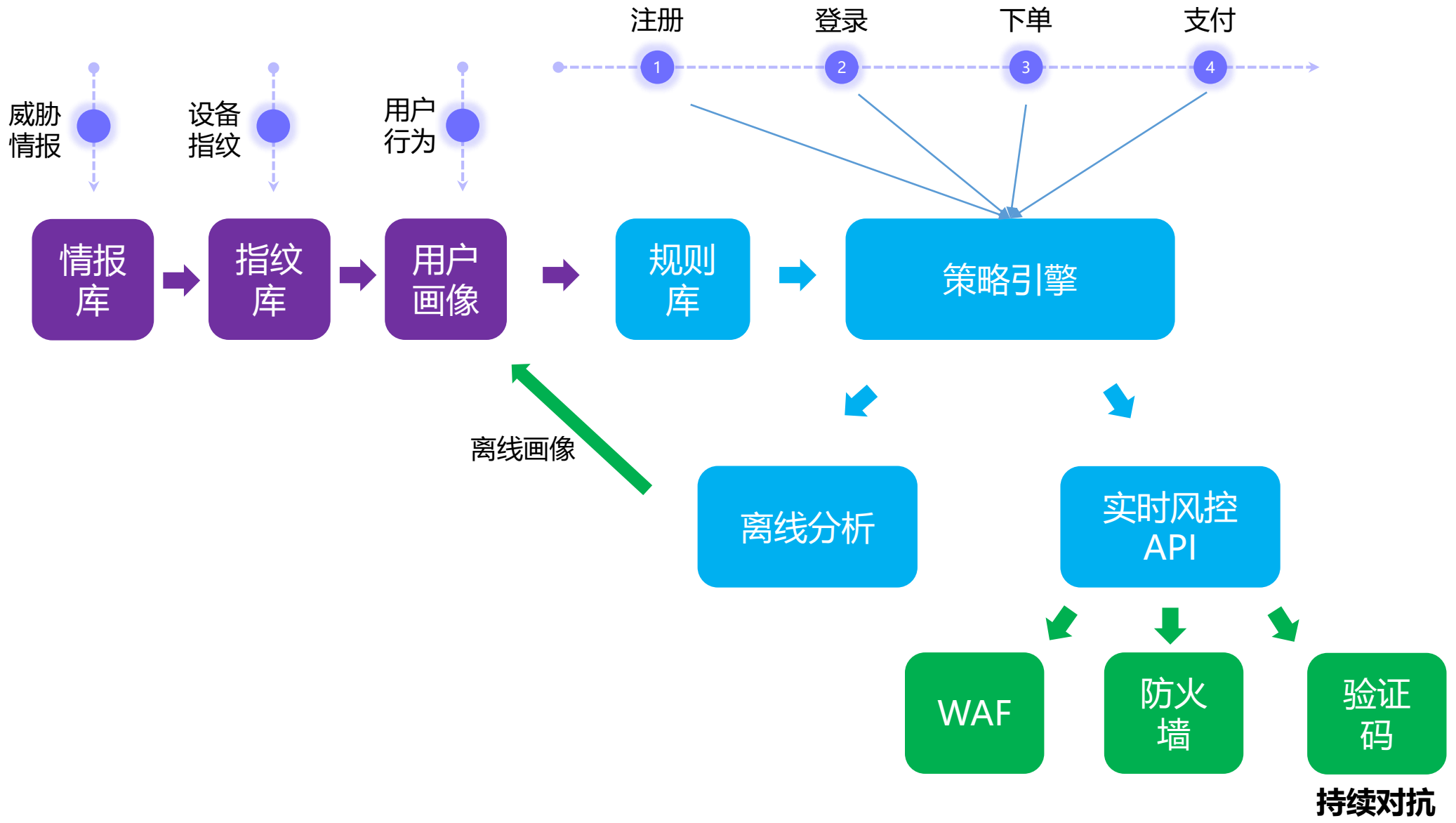
可信计算：客服场景零信任安全方案落地

数篷科技 DATACLOAK



03 Part Three
业务安全能力

业务数据安全：会员安全


注册
登录
下单
支付
1
2
3
4
威胁情报
设备指纹
用户行为
情报库
指纹库
用户画像
规则库
策略引擎
离线画像
离线分析
实时风控API
WAF
防火墙
验证码
持续对抗

04 Part Four
安全合规

安全合规技术规范

- 个人信息安全规范
- 数据出境
- APP安全合规
- 电商法
- 互联网行业要求
- 旅游行业要求
- PCI/DSS
- ISO27001
- 等级保护
- GDPR

……

提炼、归类、合并、评测

60%一致

+

40%不一致

=

安全合规技术规范

等级保护落地

对象分级保护

网络基础设施、信息系统、大数据、云平台、移动互联网、行业控制系统

网络安全综合防御

- 风险/漏洞管理系统
- 预警/审计系统
- 网络/权限管控系统
- 安全技术能力

安全管理中心

- 数据安全平台
- 业务安全平台
- 安全门户
- 安全制度、流程、基线

安全组织运营

- 安全管理委员会
- 安全应急小组
- 安全专项治理小组

全面梳理系统范围和边界
通过等级保护工作推进网络安全防护手段和安全规范要求落地

APP 安全认证

认证要求：《个人信息安全规范》（GB/T 35273）

核心要求点
五、个人信息收集收集 24个检查项，隐私政策，收集信息提示等
六、个人信息的保存 8个检查项，信息存储、删除、匿名化等
七、个人信息的使用 25个检查项，信息访问、大数据、个性化展示等
八、个人信息的委托处理、共享、转让、公开披露 30个检查项，第三方、跨境、公开等
九、个人信息安全事件处理 7个检查项，事件管理、演练、上报等
十、组织管理要求 24个检查项。组织、人员、评估、审计等

隐私政策

独立、易读
功能及收集信息类型
个人信息处理规则
免责声明

APP功能

隐私协议弹窗
权限：明示目的、方式、范围
不得捆绑和强制授权
非必要功能处理
第三方SDK

制度记录

管理制度
事件处置
个人信息影响评估
安全审计
第三方安全协议

05 Part Five
生态安全

生态安全

生态安全

感知

- 生态数据传输动态监控
- 数字水印，数据染色

防护

- 可信计算，定义信任边界
- 数据，文件加密
- 终端安全

赋能

- 生态应急响应中心
- 生态情报共享
- 安全能力输出

展望

- CARTA - inspired vulnerability management
- SOAR
- 网络空间测绘
- CASB
- Container Security
- RASP

加好友时请注明所在机构和姓名

THANKS

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE